Naam: _____ Datum: _____ Score: _____

Beveiliging van Surfshark

Onderzoek de beveiligingsfuncties van Surfshark, waaronder CleanWeb-advertentieblokkering, dynamische MultiHop-routering, de Nexus SDN-architectuur, een serverpark met uitsluitend RAM en de Camouflage-modus.

LEEROVERZICHT: BEVEILIGING VAN SURFSHARK

LEERLING
STUDENTENSTATUS
Network Defender-traject

VEILIG
VERBINDINGSSTATUS
Gegevenspakketten afschermen

ACTIEF
LEKBESCHERMING
Bescherming tegen DNS- en IPv6-lekken

Welkom! Dit activiteitenpakket leidt je door de beveiligingsarchitectuur van Surfshark. Je verkent RAM-only serverhardware, dynamische IP-rotatie via Nexus SDN, CleanWeb-advertentieblokkers en MultiHop-routering.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers VPN- en netwerkbeveiligingsconfiguraties.**
- [ ] **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-gids met de beste VPN's

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

Jouw leertraject: beveiliging van Surfshark

- Analyseer de technische architectuur en configuratieregels van Surfshark Security.
- Configureer clientinstellingen om lekken van IP-, DNS- en WebRTC-verkeer te voorkomen.
- Vergelijk aangepaste prijzen, proefperiodes en prestatiefuncties met standaardmodellen.

INSTRUCTIES VOOR DE BEVEILIGINGSGIDS VAN SURFSHARK

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 infrastructuur met alleen RAM, Nexus SDN en CleanWeb. Sluit af met de bonusopdracht Snel denken.

RAM-ONLY SERVERPARK, NEXUS SDN EN CLEANWEB-ARCHITECTUUR (INLEIDING)

Surfshark beschermt de privacy van gebruikers met een serverpark dat volledig uit RAM-only servers bestaat, software-defined networking via Nexus met IP Rotator, advertentieblokkering met CleanWeb en dynamische MultiHop-versleutelingspaden.

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

Controlepunt 1: Meerkeuzeopdracht

1. Hoe heet de geïntegreerde advertentie- en malwareblokkering van Surfshark?

- A) AdGuard
- B) CleanWeb
- C) ThreatShield
- D) NetBlocker

2. Welke hardwarearchitectuur gebruikt Surfshark op al zijn servers?

- A) Harde schijven
- B) 100% alleen RAM
- C) Optische opslag
- D) Magneetband

3. Welke functie leidt verkeer via twee verschillende VPN-servers?

- A) Bypasser
- B) MultiHop (dubbele VPN)
- C) Nexus-netwerk
- D) Statisch IP-adres

4. Welke obfuscatiefunctie vermomt VPN-verkeer als gewone webdata?

- A) Kill switch
- B) Camouflagemodus
- C) CleanWeb 2.0
- D) Split tunnel

5. Wat is de functie van het hulpmiddel Bypasser van Surfshark?

- A) Speed Booster
- B) Split tunneling
- C) Wachtwoordmanager
- D) DNS-resolver

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. RAM-only servers wissen alle operationele gegevens direct bij een herstart van de server.

○ Waar ○ Onwaar

7 Vraag 7

7. De Camouflage-modus voorkomt dat isp's ontdekken dat je een VPN gebruikt.

○ Waar ○ Onwaar

8 Vraag 8

8. CleanWeb 2.0 werkt binnen browserextensies om pop-ups voor cookietoestemming te blokkeren.

○ Waar ○ Onwaar

9 Vraag 9

9. Surfshark bewaart tijdelijke tijdstempels van verbindingen en logboeken van bandbreedtegebruik.

○ Waar ○ Onwaar

10 Vraag 10

10. Het Nexus-netwerk wisselt periodiek de IP-adressen van gebruikers zonder de verbinding te verbreken.

○ Waar ○ Onwaar

Controlepunt 3: Kernbegrippen invullen

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

1. Vervelende webadvertenties, trackingscripts en phishinglinks worden geblokkeerd door de filters van _____ .

2. Gebruikersactiviteit laat geen forensisch spoor na omdat servers werken met geheugen van het type _____ .

3. Het routeren van data via twee afzonderlijke versleutelde serversprongen gebeurt met tunnels van _____ .

4. Om het VPN-gebruik voor internetproviders te verbergen, activeren gebruikers de modus _____ .

5. Het laten omzeilen van de VPN-tunnel door bankapps wordt beheerd met de instellingen van _____ .

6. De SDN-architectuur van de volgende generatie die de serverpark verbindt, is het systeem _____ .

WOORDENBANK

BYPASSER CAMOUFLAGE CLEANWEB IP-ROTATIE KILL SWITCH MULTI-HOP NEXUS RAM-ONLY

Schrijf hier je antwoorden:

1. 2.

3. 4.

5. 6.

Controlepunt 4: VPN- en netwerkbegrippen koppelen

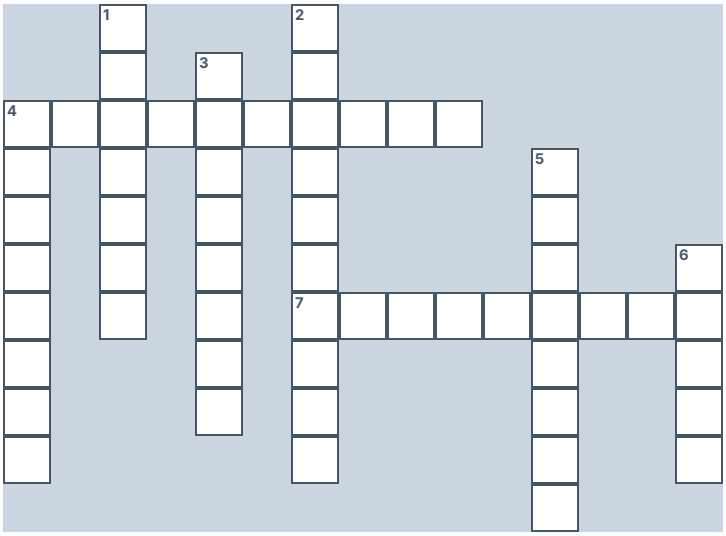
DEFINITIES KOPPELEN

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. CLEANWEB	A	Een automatische veiligheidsfunctie die netwerkverkeer blokkeert wanneer de VPN wegvalt.
☐	2. RAM-ONLY	B	Split tunneling-functionaliteit waarmee geselecteerde applicaties de VPN kunnen omzeilen.
☐	3. MULTI-HOP	C	Een geavanceerd filter dat advertenties, malware en cookietoestemmingsbanners blokkeert.
☐	4. CAMOUFLAGE	D	Serverhardware met vluchtig geheugen die bij elke aan-uitcyclus alle gegevens wist.
☐	5. OMZEILER	E	Een functie die je externe IP-adres regelmatig wijzigt zonder tunnels te onderbreken.
☐	6. KILL SWITCH	F	Obfuscatietechnologie die VPN-kenmerken verbergt zodat het lijkt op gewoon HTTPS-verkeer.
☐	7. NEXUS-NET	G	Een double-VPN-routeringsfunctie die verkeer versleutelt via twee verschillende servernodes.
☐	8. ROTEREND	H	Een eigen softwaregedefinieerd netwerk dat alle servers verbindt tot één samenhangend mesh.

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. Obfuscatietechnologie die VPN-handtekeningen verbergt om gewoon HTTPS-verkeer na te bootsen (10)

7. Een functie die je externe IP-adres regelmatig wijzigt zonder tunnels te onderbreken (9)

VERTICAAL

1. Serverhardware met vluchtig geheugen die bij elke stroomcyclus alle gegevens wist (7)

2. Een automatische veiligheidsfunctie die netwerkverkeer blokkeert als de VPN wegvalt (10)

3. Een dubbele VPN-routeringsfunctie die verkeer versleutelt via twee afzonderlijke servernodes (8)

4. Een geavanceerd filter dat advertenties, malware en cookiebanners blokkeert (8)

5. Split-tunnelingfunctie waarmee geselecteerde applicaties de VPN omzeilen (8)

6. Een eigen softwaregedefinieerd netwerk dat alle servers tot één geheel verbindt (5)

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: Obfuscatietechnologie die VPN-handtekeningen verbergt om gewoon HTTPS-verkeer na te bootsen (10 letters):

7 horizontaal: Een functie die je externe IP-adres regelmatig wijzigt zonder tunnels te onderbreken (9 letters):

VERTICAAL

1 verticaal: Serverhardware met vluchtig geheugen die bij elke stroomcyclus alle gegevens wist (7 letters):

2 verticaal: Een automatische veiligheidsfunctie die netwerkverkeer blokkeert als de VPN wegvalt (10 letters):

3 verticaal: Een dubbele VPN-routeringsfunctie die verkeer versleutelt via twee afzonderlijke servernodes (8 letters):

4 verticaal: Een geavanceerd filter dat advertenties, malware en cookiebanners blokkeert (8 letters):

5 verticaal: Split-tunnelingfunctie waarmee geselecteerde applicaties de VPN omzeilen (8 letters):

6 verticaal: Een eigen softwaregedefinieerd netwerk dat alle servers tot één geheel verbindt (5 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 U M J B D I N N
H K Q P G M M L Q R Y S T T G
C C S Q O H S T B W P D S Z V
T S C Z W C F I K H A Z D I N
I U D Q X A P H C U S B A P Z
W X N D K M A O C D S O D R F
S E H I D O R P L R E Q M O E
L N I R Z U S F E A R Q V T F
L A A Q O F N P A M T X Q A K
I R U S D L N Y N O B F S T X
K W J A R A Z Y W N Y L G I I
M R J M L G T O E L H Q Q E H
Z A O V G E U B B Y Y R Y B H
L Z G J O P N W C M Z Y G Y O

WOORDENLIJST

CLEANWEB RAMONLY MULTIHOP NEXUS CAMOUFLAGE IPROTATIE BYPASSER KILLSWITCH

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. CLEANWEB**
- **B. RAMONLY**
- **C. MULTIHOP**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. IPROTATIE**

DEFINITIES EN KOPPELVELDEN

1. Obfuscatietechnologie die VPN-handtekeningen verbergt om gewoon HTTPS-verkeer na te bootsen.
2. Een automatische veiligheidsfunctie die netwerkverkeer blokkeert als de VPN wegvalt.
3. Een geavanceerd filter dat advertenties, malware en cookiebanners blokkeert.
4. Split-tunnelingfunctie waarmee geselecteerde applicaties de VPN omzeilen.
5. Serverhardware met vluchtig geheugen die bij elke stroomcyclus alle gegevens wist.
6. Een functie die je externe IP-adres regelmatig wijzigt zonder tunnels te onderbreken.
7. Een dubbele VPN-routeringsfunctie die verkeer versleutelt via twee afzonderlijke servernodes.
8. Een eigen softwaregedefinieerd netwerk dat alle servers tot één geheel verbindt.

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen van Virtual Private Networks (VPN) te onthullen. Schrijf je antwoorden in de invulvelden.

1. **EANCWLBE** _____
2. **TMPUOHIL** _____
3. **AYBSSREP** _____
4. **XSUNE** _____
5. **NYOMRLA** _____
6. **GUOLACAFEM** _____
7. **ILKIWTCHSL** _____
8. **ETIIOPATR** _____

Bonusopdracht: Snel denken

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

1	Beveiligingsfuncties in Surfshark			
2	Tekenen dat je VPN-verbinding traag is			
3	VPN-protocollen die je kent			
4	Dingen die versleuteling beschermt			
5	Bedreigingen op openbare wifi			
6	Landen die bekendstaan om sterke privacywetten			
7	Manieren om een sterk wachtwoord te maken			
8	Apparaten waarop je Surfshark zou installeren			
9	Vragen voor de klantenservice van Surfshark			
10	Instellingen die je aanzet voor extra beveiliging			
11	Dingen die Surfshark voor je netwerk kan verbergen			
12	Soorten VPN-lekken			
13	Gegevens die een VPN nooit zou mogen opslaan			
14	Woorden die een goede VPN-app beschrijven			
15	Dingen die een audit kan controleren			

Controlepunt 8: Casestudy's VPN en netwerk

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

CASESTUDY 1: FILTERS OP CAMPUS EN WERKPLEK OMZEILEN



Scenario: Een student ontdekt dat het wifinetwerk van zijn universiteitscampus alle standaard OpenVPN- en WireGuard-poorten blokkeert.

Discussievraag: Welke functie van Surfshark stelt de student in staat verbinding te maken zonder dat netwerkbeheerders dit detecteren?

CASESTUDY 2: JOURNALISTIEK ONDERZOEK MET HOOG RISICO



Scenario: Een onderzoeksjournalist heeft extra bescherming tegen surveillance nodig tijdens het onderzoeken van gevoelige bedrijfsgegevens.

Discussievraag: Hoe biedt Dynamic MultiHop betere privacy dan routering via één server?

Controlepunt 9: De code ontcijferen

Een netwerkingenieur beveiligt routeringskanalen en clienttunnels. Gebruik de onderstaande letter-naar-cijfersleutel om het bericht te ontcijferen door de bijbehorende letters in de lege vakjes te schrijven.

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

19	21	18	6	19	8	1	18	11		14	5	24	21	19		5	14		9	16
18	15	20	1	20	9	5		22	5	18	19	20	5	18	11	5	14			
							16	18	9	22	1	3	25							

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 over virtuele privénetwerken (VPN's) en tunneling.

Q1: Wat is Surfshark CleanWeb?

CleanWeb is een geïntegreerde beveiligingsfunctie die advertenties, trackers, malware en phishingsites blokkeert.

Q2: Wat zijn RAM-only-servers?

RAM-only servers draaien op vluchtig geheugen, wat betekent dat gegevens in het geheugen worden gewist wanneer servers opnieuw opstarten.

Q3: Wat is Surfshark MultiHop?

MultiHop (Double VPN) routeert en versleutelt je internetverbinding via twee verschillende serverlocaties.

Q4: Hoe werkt Camouflage Mode?

De Camouflage-modus verhult VPN-verkeer, zodat je isp niet kan zien dat je een VPN gebruikt.

Q5: Wat is de Bypasser-functie?

Bypasser is de split-tunnelingtool van Surfshark waarmee specifieke apps of websites de VPN kunnen omzeilen.

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

Bekijk de meestgestelde vragen en antwoorden over virtuele privénetwerken (VPN's) en tunneling.

Q6: Heeft Surfshark een Kill Switch?

Ja, de Kill Switch verbreekt je internetverbinding als de VPN onverwacht wegvalt.

Q7: Welke versleutelingsstandaard gebruikt Surfshark?

Surfshark gebruikt AES-256-GCM en ChaCha20, plus AEGIS-256X2 in het nieuwe Dausos-protocol.

Q8: Is het no-logsbeleid van Surfshark geaudit?

Ja, Deloitte heeft het no-logsbeleid van Surfshark in 2023 en opnieuw in 2025 geverifieerd.

Q9: Wat is Surfshark Nexus?

Nexus is een geavanceerde SDN-architectuur die alle servers verbindt tot één geïntegreerd netwerk voor soepelere routering.

Q10: Wat is de functie IP Rotator?

IP Rotator verandert je IP-adres automatisch om de paar minuten zonder je VPN-sessie te verbreken.

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

Verken geavanceerde technische aspecten van VPN-tunnelprotocollen, integraties van mobiele clients en implementatie in bedrijven.

Q1: Waarin verschilt Dynamic MultiHop van traditionele dubbele VPN?

Met Dynamic MultiHop kun je elke combinatie van ingangs- en uitgangsservers wereldwijd aanpassen.

Q2: Werkt CleanWeb 2.0 in browserextensies?

Ja, CleanWeb 2.0 blokkeert videoadvertenties, pop-ups voor cookietoestemming en meldingsbanners in Chrome/Firefox.

Q3: Wat is Alternative ID in de beveiligingssuite?

Alternative ID genereert unieke persoonlijke pseudoniemen, e-mailadressen en telefoonmaskers.

Q4: Hoe voorkomt Surfshark DNS-lekken?

Surfshark routeert alle domeinverzoeken via zijn eigen privé-DNS-servers op elke node.

Q5: Ondersteunt Surfshark ChaCha20-versleuteling op mobiel?

Ja, WireGuard op Android en iOS gebruikt ChaCha20-Poly1305 voor superieure efficiëntie op mobiele apparaten.

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

Verken geavanceerde technische aspecten van VPN-tunnelprotocollen, integraties van mobiele clients en implementatie in bedrijven.

Q6: Wat is de NoBorders-modus in Surfshark?

NoBorders detecteert automatisch beperkende netwerkomgevingen en levert gespecialiseerde servers.

Q7: Wie heeft de beveiligingsaudits van de browserextensies van Surfshark uitgevoerd?

Het onafhankelijke cyberbeveiligingsbureau Cure53 heeft audits uitgevoerd op browserextensies en serversystemen.

Q8: Hoe beschermt Surfshark tegen IPv6-lekken?

Surfshark routeert IPv6-verkeer veilig of beperkt het veilig om onversleutelde lekken te voorkomen.

Q9: Waar is het rechtsgebied van Surfshark gevestigd?

Surfshark opereert onder Nederlands recht en houdt zich aan de strenge Europese privacynormen van de AVG (GDPR).

Q10: Ondersteunt Surfshark tweefactorauthenticatie (2FA)?

Ja, en Surfshark One voegt een 2FA-vergrendeling toe, zodat alleen jij de functie-instellingen kunt wijzigen.

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

Bekijk feiten uit de praktijk over VPN-versleutelingssnelheden, protocolaudits, mobiele connectiviteit en zakelijk werken op afstand.

1. VPN-INZICHT

1. Surfshark zegt dat het hele netwerk van meer dan 4.500 servers draait op schijfloze, vluchtige hardware die alleen RAM gebruikt.

2. VPN-INZICHT

2. Het Big Four-bedrijf Deloitte heeft het no-logsbeleid van Surfshark in 2023 en opnieuw in november 2025 geverifieerd.

3. VPN-INZICHT

3. De eigen Nexus-architectuur verbindt alle wereldwijde servers tot een dynamisch softwaregedefinieerd netwerk.

4. VPN-INZICHT

4. Rotating IP wijzigt je IP-adres ongeveer elke vijf minuten zonder dat de VPN-verbinding wegvalt.

5. VPN-INZICHT

5. CleanWeb 2.0 blokkeert opdringerige cookietoestemmings-pop-ups en videoadvertenties rechtstreeks in browsers.

6. VPN-INZICHT

6. Met Dynamic MultiHop kunnen gebruikers aangepaste versleutelingspaden met twee servers maken in 100 landen.

7. VPN-INZICHT

7. Camouflagemodus verwijdert de VPN-headerkenmerken, waardoor verkeer niet te onderscheiden is van gewoon HTTPS.

8. VPN-INZICHT

8. Alternative ID genereert wegwerppseudoniemen en e-mailmaskers om gebruikers te beschermen tegen datalekken.

9. VPN-INZICHT

9. Surfshark past symmetrische AES-256-GCM-versleuteling toe naast ChaCha20 op WireGuard-protocollen.

10. VPN-INZICHT

10. De NoBorders-modus wordt automatisch ingeschakeld op beperkte netwerken om veerkrachtige tunneltoegang te bieden.

Technische referenties en bronnen

De studiegids en de interactieve puzzels zijn samengesteld uit wereldwijde technische standaarden, specificaties en regelgevend kaders.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[1] Surfshark. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 **Geïntegreerde contentblocker** VERDEDIGING TEGEN ADVERTENTIES EN MALWARE **Juist antwoord: B**

DOCENTENNOTITIE

CleanWeb is het geïntegreerde beveiligingsfilter van Surfshark dat advertenties, trackerdomeinen, phishingwebsites en kwaadaardige URL-scripts op netwerkniveau blokkeert. Bron: CleanWeb Security Specs.

2 **100% infrastructuur die alleen op RAM draait** RAM-ARCHITECTUUR **Juist antwoord: B**

DOCENTENNOTITIE

Surfshark gebruikt RAM-only servers, dus gegevens in het servergeheugen worden gewist wanneer een server wordt uitgeschakeld of opnieuw opgestart. Bron: Cure53 Infrastructure Audit.

3 **MultiHop-dubbeltunneling** MULTIHOP-VPN **Juist antwoord: B**

DOCENTENNOTITIE

MultiHop (Double VPN) versleutelt verkeer via twee afzonderlijke servernodes in verschillende landen om correlatieaanvallen op verkeer te voorkomen. Bron: Surfshark MultiHop Guide.

4 **Obfuscatie met de Camouflage-modus** OBFUSCATIE **Juist antwoord: B**

DOCENTENNOTITIE

De Camouflage-modus past OpenVPN-pakketheaders aan om VPN-verkeer te vermommen als standaard HTTPS-verkeer, waardoor restrictieve firewallblokkades worden omzeild. Bron: Surfshark Stealth Whitepaper.

5 **Bypasser-split tunneling** SPLIT TUNNELING **Juist antwoord: B**

DOCENTENNOTITIE

Bypasser is de split-tunnelingtool van Surfshark waarmee gebruikers specifieke apps of websites kunnen kiezen die rechtstreeks via hun gewone verbinding met de internetprovider worden gerouteerd. Bronvermelding: Surfshark Client Features.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Wissen van gegevens in vluchtig geheugen**

SERVERBEVEILIGING

Juist antwoord: Waar

DOCENTENNOTITIE

RAM-only servers slaan geen gegevens op permanente harde schijven op; bij een herstart van de hardware wordt al het operationele geheugen direct gewist. Bron: RAM Server Architecture.

7 **Camouflage-modus voor het verbergen van VPN-gebruik voor de isp**

VERBERGEN VAN VERKEER

Juist antwoord: Waar

DOCENTENNOTITIE

De Camouflage-modus verwijdert de protocolkenmerken van OpenVPN, zodat isp's niet kunnen ontdekken dat de gebruiker verbonden is met een VPN-tunnel. Bron: Deep Packet Inspection Guide.

8 **CleanWeb 2.0-browserextensies**

BROWSEREXTENSIE

Juist antwoord: Waar

DOCENTENNOTITIE

CleanWeb 2.0 werkt binnen browserextensies om pop-ups voor cookietoestemming, videoadvertenties en kwaadaardige redirectscripts in realtime te blokkeren. Bron: CleanWeb 2.0 Release Notes.

9 **Geen bewaring van verbindingslogs**

NO-LOGSBELEID

Juist antwoord: Onwaar

DOCENTENNOTITIE

Surfshark hanteert een strikt, onafhankelijk geaudit zero-logsbeleid en registreert geen IP-adressen, tijdstempels van verbindingen of bandbreedtelogboeken. Bron: Deloitte No-Logs Audit.

10 **Dynamische IP-rotatie van Nexus**

NEXUS-NETWERK

Juist antwoord: Waar

DOCENTENNOTITIE

Het Surfshark Nexus software-defined network wisselt de IP-adressen van gebruikers dynamisch om de paar minuten, zonder de actieve VPN-verbinding te verbreken. Bron: Surfshark Nexus Architecture.

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

C 1. CLEANWEB	D 2. RAM-ONLY	G 3. MULTI-HOP	F 4. CAMOUFLAGE
B 5. OMZEILER	A 6. KILL SWITCH	H 7. NEXUS-NET	E 8. ROTEREND

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 CLEANWEB	2 RAM-ONLY	3 MULTI-HOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – RAMONLY	6 H – IPROTATIE	7 C – MULTIHOP	8 G – NEXUS

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen CLEANWEB, RAM-ONLY en MULTI-HOP 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.

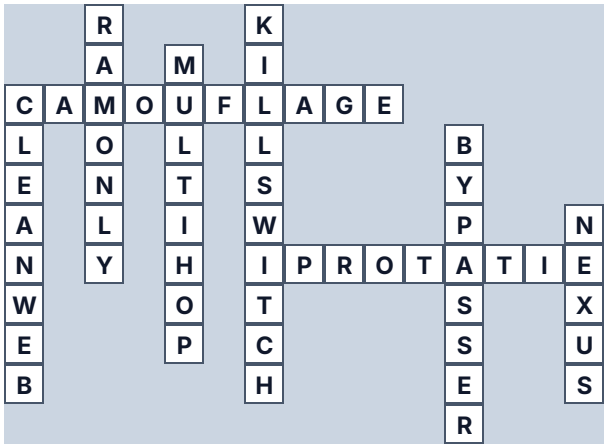
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

4 horizontaal: CAMOUFLAGE Obfuscatietechnologie die VPN-handtekeningen verbergt om gewoon HTTPS-verkeer na te bootsen (10 letters)

7 horizontaal: IPROTATIE Een functie die je externe IP-adres regelmatig wijzigt zonder tunnels te onderbreken (9 letters)

VERTICAAL

1 verticaal: RAMONLY Serverhardware met vluchtig geheugen die bij elke stroomcyclus alle gegevens wist (7 letters)

2 verticaal: KILLSWITCH Een automatische veiligheidsfunctie die netwerkverkeer blokkeert als de VPN wegvalt (10 letters)

3 verticaal: MULTIHOP Een dubbele VPN-routeringsfunctie die verkeer versleutelt via twee afzonderlijke servernodes (8 letters)

4 verticaal: CLEANWEB Een geavanceerd filter dat advertenties, malware en cookiebanners blokkeert (8 letters)

5 verticaal: BYPASSER Split-tunnelingfunctie waarmee geselecteerde applicaties de VPN omzeilen (8 letters)

6 verticaal: NEXUS Een eigen softwaregedefinieerd netwerk dat alle servers tot één geheel verbindt (5 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. EANCWLBE — **CLEANWEB**
2. TMPUOHIL — **MULTIHOP**
3. AYBSSREP — **BYPASSER**
4. XSUNE — **NEXUS**
5. NYOMRLA — **RAMONLY**
6. GUOLACAFEM — **CAMOUFLAGE**
7. ILKIWTCHSL — **KILLSWITCH**
8. ETIIOPATR — **IPROTATIE**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"SURFSHARK NEXUS EN IP ROTATIE VERSTERKEN PRIVACY"

Antwoordsleutel casestudy's

A CASESTUDY 1: FILTERS OP CAMPUS EN WERKPLEK OMZEILEN

Oplossing voor docenten

BEOORDELINGSRUBRIEK EN RICHTLIJNEN VOOR OPLOSSINGEN

- Scenarioanalyse: Een student ontdekt dat de wifi op zijn universiteitscampus alle standaardpoorten van OpenVPN en WireGuard blokkeert.
- Focusvraag: Welke Surfshark-functie laat de student verbinding maken zonder dat netwerkbeheerders dit opmerken?
- Aanbevolen strategie en oplossing: Activeer de Camouflage-modus (OpenVPN), die VPN-metadata verbergt zodat firewalls normaal HTTPS-verkeer zien.

B CASESTUDY 2: JOURNALISTIEK ONDERZOEK MET HOOG RISICO

Oplossing voor docenten

BEOORDELINGSRUBRIEK EN RICHTLIJNEN VOOR OPLOSSINGEN

- Scenarioanalyse: Een onderzoeksjournalist heeft extra bescherming tegen surveillance nodig bij het onderzoeken van gevoelige bedrijfsdossiers.
- Focusvraag: Hoe biedt Dynamic MultiHop betere privacy dan routering via één server?
- Aanbevolen strategie en oplossing: Dynamic MultiHop routeert verkeer via ingangs- en uitgangsservers in twee landen, zodat geen enkele server de gebruiker kan blootstellen.