Name: _____ Datum: _____ Punkte: _____

Sicherheit von Surfshark

Untersuchung der Sicherheitsfunktionen von Surfshark, einschließlich des Werbeblockers CleanWeb, dynamischem MultiHop-Routing, der SDN-Architektur Nexus, der RAM-only-Serverflotte und des Camouflage-Modus.

SURFSHARK-SICHERHEIT: LERNÜBERSICHT

LERNENDE
STUDIERENDENSTATUS
Lernpfad Netzwerkverteidigung

SICHER
VERBINDUNGSSTATUS
Abschirmung von Datenpaketen

AKTIV
SCHUTZ VOR LECKS
Schutz vor DNS- und IPv6-Leaks

Willkommen! Dieses Aktivitätspaket führt Sie durch die Sicherheitsarchitektur von Surfshark. Sie lernen reine RAM-Server-Hardware, dynamische IP-Rotation mit Nexus SDN, den Werbeblocker CleanWeb und MultiHop-Routing kennen.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: VPN- und Netzwerksicherheitskonfigurationen beherrschen.**
- [ ] **Teil 5-7: Kreuzworträtsel und Suchsel lösen.**
- [ ] **Teil 8-9: Fallstudien und Chiffre-Aufgabe lösen.**
- [ ] **Teil 10: Seiten mit grundlegenden und fortgeschrittenen häufigen Fragen durchgehen.**
- [ ] **Teil 11: 10 interessante Fakten aus der Praxis entdecken.**
- [ ] **Bonus: Herausforderung Schnell denken.**

Leitfaden „Beste VPNs“ von VPN.com öffnen

URL: https://www.vpn.com/de/vpn/surfshark/sicherheit/

Ihr Lernfahrplan: Surfshark-Sicherheit

- Analysieren Sie die technische Architektur und die Konfigurationsregeln von Surfshark (Sicherheit).
- Konfigurieren Sie die Client-Einstellungen so, dass IP-, DNS- und WebRTC-Leaks verhindert werden.
- Vergleichen Sie individuelle Preise, Testversionen und Leistungsmerkmale mit Standardmodellen.

SURFSHARK-SICHERHEIT: ANLEITUNG ZUM LEITFADEN

Beantworten Sie die Auswahlaufgaben und Richtig/Falsch-Fragen, vervollständigen Sie die Lückensätze mithilfe der Wortliste, ordnen Sie die Definitionen zu und lösen Sie das Kreuzworträtsel und das Suchsel. Wenden Sie Ihr Wissen in folgenden Bereichen an: Reine RAM-Infrastruktur, Nexus-SDN und CleanWeb. Zum Schluss folgt die Bonusaufgabe Schnell denken.

REINE RAM-SERVERFLOTTE, NEXUS SDN UND CLEANWEB-ARCHITEKTUR (EINFÜHRUNG)

Surfshark schützt die Privatsphäre der Nutzer durch eine Serverflotte, die ausschließlich im RAM läuft, softwaredefinierte Vernetzung mit Nexus und IP Rotator, Werbeblocker CleanWeb und dynamische MultiHop-Verschlüsselungspfade.

LESEN SIE JEDEN KONTROLLPUNKT SORGFÄLTIG UND WÄHLEN ODER SCHREIBEN SIE DIE RICHTIGE ANTWORT.

Kontrollpunkt 1: Auswahlaufgaben

1. Wie heißt der integrierte Werbe- und Malware-Blocker von Surfshark?

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

2. Welche Hardwarearchitektur nutzt Surfshark auf allen Servern?

- A) Festplattenlaufwerke
- B) 100 % reiner RAM-Betrieb
- C) Optischer Speicher
- D) Magnetband

3. Welche Funktion leitet den Datenverkehr über zwei verschiedene VPN-Server?

- A) Bypasser
- B) MultiHop (Double VPN)
- C) Nexus-Netzwerk
- D) Statische IP

4. Welche Verschleierungsfunktion tarnt VPN-Datenverkehr als normale Webdaten?

- A) Kill Switch
- B) Tarnmodus
- C) CleanWeb 2.0
- D) Split Tunnel

5. Welche Funktion hat das Tool Surfshark Bypasser?

- A) Speed Booster
- B) Split Tunneling
- C) Passwort-Manager
- D) DNS-Resolver

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Reine RAM-Server löschen beim Neustart des Servers sofort alle Betriebsdaten.

○ Richtig ○ Falsch

7 Frage 7

7. Der Camouflage-Modus verhindert, dass ISPs erkennen, dass Sie ein VPN nutzen.

○ Richtig ○ Falsch

8 Frage 8

8. CleanWeb 2.0 arbeitet in Browsererweiterungen und blockiert Cookie-Einwilligungs-Pop-ups.

○ Richtig ○ Falsch

9 Frage 9

9. Surfshark speichert vorübergehend Zeitstempel von Verbindungen und Protokolle über die Bandbreitennutzung.

○ Richtig ○ Falsch

10 Frage 10

10. Das Nexus-Netzwerk wechselt die IP-Adressen der Nutzer regelmäßig, ohne die Verbindung zu trennen.

○ Richtig ○ Falsch

Kontrollpunkt 3: Schlüsselbegriffe einsetzen

Lesen Sie jeden der folgenden Sätze und füllen Sie die Lücke mit dem richtigen Begriff aus der Wortliste.

1. Lästige Webwerbung, Tracking-Skripte und Phishing-Links werden von den Filtern von _____ blockiert.

2. Nutzeraktivitäten hinterlassen keine forensischen Spuren, weil die Server als _____ nur im Arbeitsspeicher arbeiten.

3. Die Weiterleitung von Daten über zwei getrennte verschlüsselte Server-Hops gelingt mit Tunneln per _____ .

4. Um die VPN-Nutzung vor Internetanbietern zu verbergen, aktivieren Nutzer den Modus _____ .

5. Dass Banking-Apps den VPN-Tunnel umgehen dürfen, regeln die Einstellungen von _____ .

6. Die SDN-Architektur der nächsten Generation, die die Serverflotte verbindet, ist das System _____ .

WORTSCHATZ-WORTBANK

BYPASSER CAMOUFLAGE CLEANWEB IP-ROTATION KILL SWITCH MULTI-HOP NEXUS RAM-SERVER

Schreiben Sie Ihre Antworten hier:

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

Kontrollpunkt 4: Zuordnung von VPN- und Netzwerk-Begriffen

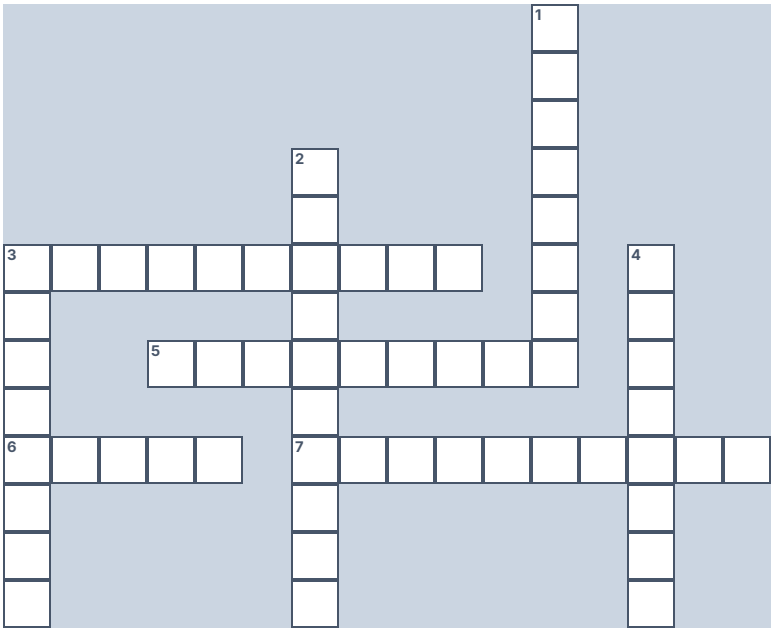
DEFINITIONEN ZUORDNEN

Ordnen Sie jeden Fachbegriff links der richtigen Definition rechts zu, indem Sie den passenden Buchstaben (A–H) in das ausfüllbare Eingabefeld schreiben.

☐	1. CLEANWEB	A	Eine automatische Sicherheitsfunktion, die den Netzwerkverkehr blockiert, wenn das VPN abbricht.
☐	2. RAM-SERVER	B	Split-Tunneling-Funktion, mit der ausgewählte Anwendungen das VPN umgehen können.
☐	3. MULTI-HOP	C	Ein erweiterter Filter, der Werbung, Malware und Cookie-Banner blockiert.
☐	4. TARNUNG	D	Serverhardware mit flüchtigem Speicher, die bei jedem Stromzyklus alle Daten löscht.
☐	5. UMGEHER	E	Eine Funktion, die Ihre externe IP-Adresse regelmäßig ändert, ohne Tunnel zu unterbrechen.
☐	6. KILL SWITCH	F	Verschleierungstechnik, die VPN-Signaturen verbirgt, um normalen HTTPS-Verkehr nachzuahmen.
☐	7. NEXUS-NETZWERK	G	Eine Double-VPN-Routingfunktion, die den Datenverkehr über zwei verschiedene Serverknoten verschlüsselt.
☐	8. ROTIEREND	H	Ein proprietäres softwaredefiniertes Netzwerk, das alle Server zu einem einheitlichen Mesh verbindet.

Kontrollpunkt 5: Kreuzworträtsel

Lösen Sie das Kreuzworträtsel, indem Sie Buchstaben in die aktiven weißen Felder eingeben. Die Zahlen entsprechen den Hinweisen unten.



WAAGERECHT

3. Verschleierungstechnik, die VPN-Signaturen verbirgt, damit der Verkehr wie normales HTTPS aussieht (10)

5. Server-Hardware mit flüchtigem Speicher, die bei jedem Stromzyklus alle Daten löscht (9)

6. Proprietäres softwaredefiniertes Netzwerk, das alle Server zu einem einheitlichen Mesh verbindet (5)

7. Funktion, die Ihre externe IP-Adresse regelmäßig ändert, ohne Tunnel zu unterbrechen (10)

SENKRECHT

1. Split-Tunneling-Funktion, mit der ausgewählte Anwendungen das VPN umgehen (8)

2. Automatische Sicherheitsfunktion, die den Netzwerkverkehr blockiert, wenn das VPN ausfällt (10)

3. Fortschrittlicher Filter, der Werbung, Malware und Cookie-Banner blockiert (8)

4. Double-VPN-Funktion, die den Datenverkehr über zwei verschiedene Serverknoten verschlüsselt (8)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

Nutzer von Screenreadern und Tastatur können die Kreuzworträtsel-Antworten direkt in die Textfelder unten eingeben.

WAAGERECHT

3 waagerecht: Verschleierungstechnik, die VPN-Signaturen verbirgt, damit der Verkehr wie normales HTTPS aussieht (10 Buchstaben):

5 waagerecht: Server-Hardware mit flüchtigem Speicher, die bei jedem Stromzyklus alle Daten löscht (9 Buchstaben):

6 waagerecht: Proprietäres softwaredefiniertes Netzwerk, das alle Server zu einem einheitlichen Mesh verbindet (5 Buchstaben):

7 waagerecht: Funktion, die Ihre externe IP-Adresse regelmäßig ändert, ohne Tunnel zu unterbrechen (10 Buchstaben):

SENKRECHT

1 senkrecht: Split-Tunneling-Funktion, mit der ausgewählte Anwendungen das VPN umgehen (8 Buchstaben):

2 senkrecht: Automatische Sicherheitsfunktion, die den Netzwerkverkehr blockiert, wenn das VPN ausfällt (10 Buchstaben):

3 senkrecht: Fortschrittlicher Filter, der Werbung, Malware und Cookie-Banner blockiert (8 Buchstaben):

4 senkrecht: Double-VPN-Funktion, die den Datenverkehr über zwei verschiedene Serverknoten verschlüsselt (8 Buchstaben):

Kontrollpunkt 6: Suchsel

Finden Sie die 8 wichtigen Fachbegriffe, die im Gitter unten versteckt sind. Die Wörter können waagerecht, senkrecht oder diagonal verlaufen.

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

WORTSCHATZ-WORTLISTE

CLEANWEB RAMSERVER MULTIHOP NEXUS CAMOUFLAGE IPROTATION BYPASSER KILLSWITCH

Kontrollpunkt 6, Alternative: Barrierefreie Begriffszuordnung

Ordnen Sie jeden der 8 Fachbegriffe aus dem Suchrätsel der richtigen Definition zu, indem Sie den Buchstaben (A–H) in die Lücke schreiben.

FACHBEGRIFFE

- **A. CLEANWEB**
- **B. RAMSERVER**
- **C. MULTIHOP**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. IPROTATION**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Verschleierungstechnik, die VPN-Signaturen verbirgt, damit der Verkehr wie normales HTTPS aussieht.

_____ 2. Automatische Sicherheitsfunktion, die den Netzwerkverkehr blockiert, wenn das VPN ausfällt.

_____ 3. Fortschrittlicher Filter, der Werbung, Malware und Cookie-Banner blockiert.

_____ 4. Split-Tunneling-Funktion, mit der ausgewählte Anwendungen das VPN umgehen.

_____ 5. Server-Hardware mit flüchtigem Speicher, die bei jedem Stromzyklus alle Daten löscht.

_____ 6. Funktion, die Ihre externe IP-Adresse regelmäßig ändert, ohne Tunnel zu unterbrechen.

_____ 7. Double-VPN-Funktion, die den Datenverkehr über zwei verschiedene Serverknoten verschlüsselt.

_____ 8. Proprietäres softwaredefiniertes Netzwerk, das alle Server zu einem einheitlichen Mesh verbindet.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale Begriffe zu Virtual Private Networks (VPN) aufzudecken. Schreiben Sie Ihre Antworten in die vorgesehenen Eingabefelder.

1. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. VEARRSREM
6. GUOLACAFEM
7. ILKIWTCHSL
8. OOANITPTIR

Bonusaufgabe: Schnell denken

3 ANTWORTEN PRO KATEGORIE. WER DIE LISTE ZUERST VOLLSTÄNDIG AUSFÜLLT, GEWINNT.

1	Sicherheitsfunktionen von Surfshark			
2	Anzeichen, dass Ihre VPN-Verbindung langsam ist			
3	VPN-Protokolle, die Sie kennen			
4	Dinge, die Verschlüsselung schützt			
5	Bedrohungen in öffentlichen WLANs			
6	Länder, die für strenge Datenschutzgesetze bekannt sind			
7	Möglichkeiten, ein starkes Passwort zu erstellen			
8	Geräte, auf denen Sie Surfshark installieren würden			
9	Fragen an den Kundensupport von Surfshark			
10	Einstellungen, die Sie für mehr Sicherheit einschalten			
11	Dinge, die Surfshark vor Ihrem Netzwerk verbergen kann			
12	Arten von VPN-Lecks			
13	Daten, die ein VPN niemals speichern sollte			
14	Wörter, die eine gute VPN-App beschreiben			
15	Dinge, die ein Audit prüfen kann			

Kontrollpunkt 8: Fallstudien zu VPN und Netzwerken

Wenden Sie die erlernten Konzepte an, um die folgenden praxisnahen Szenarien zu lösen.

FALLSTUDIE 1: UMGEHUNG VON FILTERN AN HOCHSCHULE UND ARBEITSPLATZ

👷

Szenario: Ein Student stellt fest, dass das WLAN auf seinem Universitätscampus alle üblichen OpenVPN- und WireGuard-Ports blockiert.

Diskussionsfrage: Mit welcher Surfshark-Funktion kann sich der Student verbinden, ohne von den Netzwerkadministratoren entdeckt zu werden?

FALLSTUDIE 2: JOURNALISTISCHE RECHERCHE MIT HOHEM RISIKO

👷

Szenario: Eine investigative Journalistin braucht zusätzlichen Schutz vor Überwachung, während sie zu sensiblen Unternehmensunterlagen recherchiert.

Diskussionsfrage: Wie bietet Dynamic MultiHop im Vergleich zur Weiterleitung über einen einzelnen Server mehr Privatsphäre?

Kontrollpunkt 9: Entschlüsselung der Chiffre

Eine Netzwerktechnikerin oder ein Netzwerktechniker sichert Routing-Kanäle und Client-Tunnel. Entschlüsseln Sie mithilfe des Buchstaben-Zahlen-Schlüssels unten die Nachricht, indem Sie die passenden Buchstaben in die Lücken schreiben.

SCHLÜSSEL FÜR DIE BUCHSTABEN-ZAHLEN-VERSCHLÜSSELUNG

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

14	5	24	21	19		9	16		18	15	20	1	20	9	15	14

19	20	1	5	18	11	20		4	9	5

16	18	9	22	1	20	19	16	8	1	5	18	5

Entschlüsselte Nachricht:

TIPP: JEDE ZAHL STEHT FÜR DIE POSITION DIESES BUCHSTABENS IM ALPHABET (Z. B. 1 = A, 2 = B, 26 = Z).

Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil A)

Sehen Sie sich die häufigsten Fragen und Antworten zu virtuellen privaten Netzwerken (VPNs) und Tunneling an.

Q1: Was ist Surfshark CleanWeb?

CleanWeb ist eine integrierte Sicherheitsfunktion, die Werbung, Tracker, Malware und Phishing-Websites blockiert.

Q2: Was sind reine RAM-Server?

Reine RAM-Server laufen auf flüchtigem Speicher, d. h. die im Speicher gehaltenen Daten werden bei jedem Neustart der Server gelöscht.

Q3: Was ist Surfshark MultiHop?

MultiHop (Double VPN) leitet und verschlüsselt Ihre Internetverbindung über zwei verschiedene Serverstandorte.

Q4: Wie funktioniert der Camouflage-Modus?

Der Camouflage-Modus verschleiert VPN-Datenverkehr, sodass Ihr ISP nicht erkennen kann, dass Sie ein VPN nutzen.

Q5: Was ist die Bypasser-Funktion?

Bypasser ist das Split-Tunneling-Werkzeug von Surfshark, mit dem bestimmte Apps oder Websites das VPN umgehen können.

Kontrollpunkt 10: Grundlegende häufige Fragen zu VPN (Teil B)

Sehen Sie sich die häufigsten Fragen und Antworten zu virtuellen privaten Netzwerken (VPNs) und Tunneling an.

Q6: Hat Surfshark einen Kill Switch?

Ja, der Kill Switch trennt Sie vom Internet, wenn das VPN unerwartet abbricht.

Q7: Welchen Verschlüsselungsstandard verwendet Surfshark?

Surfshark verwendet AES-256-GCM und ChaCha20 sowie bei seinem neuen Dausos-Protokoll AEGIS-256X2.

Q8: Wurde die No-Logs-Richtlinie von Surfshark geprüft?

Ja, Deloitte hat die No-Logs-Richtlinie von Surfshark 2023 und erneut 2025 bestätigt.

Q9: Was ist Surfshark Nexus?

Nexus ist eine fortschrittliche SDN-Architektur, die alle Server für ein reibungsloseres Routing zu einem einheitlichen Netzwerk verbindet.

Q10: Was ist die Funktion IP Rotator?

IP Rotator ändert Ihre IP-Adresse automatisch alle paar Minuten, ohne Ihre VPN-Sitzung zu trennen.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil C)

Erkunden Sie fortgeschrittene technische Aspekte von VPN-Tunnelprotokollen, der Integration mobiler Clients und des Einsatzes in Unternehmen.

Q1: Wie unterscheidet sich Dynamic MultiHop vom klassischen Double VPN?

Mit Dynamic MultiHop können Sie beliebige Kombinationen aus Eingangs- und Ausgangsservern weltweit zusammenstellen.

Q2: Funktioniert CleanWeb 2.0 mit Browsererweiterungen?

Ja, CleanWeb 2.0 blockiert Videoanzeigen, Cookie-Einwilligungs-Pop-ups und Hinweisbanner in Chrome/Firefox.

Q3: Was ist Alternative ID in der Sicherheitssuite?

Alternative ID erzeugt eindeutige persönliche Pseudonyme, E-Mail-Adressen und Telefonnummern-Masken.

Q4: Wie verhindert Surfshark DNS-Lecks?

Surfshark leitet alle Domain-Anfragen über eigene private DNS-Server auf jedem Knoten.

Q5: Unterstützt Surfshark auf Mobilgeräten die ChaCha20-Verschlüsselung?

Ja, WireGuard nutzt unter Android und iOS ChaCha20-Poly1305 für eine besonders hohe Effizienz auf Mobilgeräten.

Kontrollpunkt 10: Fortgeschrittene häufige Fragen zu VPN (Teil D)

Erkunden Sie fortgeschrittene technische Aspekte von VPN-Tunnelprotokollen, der Integration mobiler Clients und des Einsatzes in Unternehmen.

Q6: Was ist der NoBorders-Modus in Surfshark?

NoBorders erkennt automatisch restriktive Netzwerkumgebungen und stellt spezielle Server bereit.

Q7: Wer hat die Sicherheitsaudits der Browsererweiterungen von Surfshark durchgeführt?

Das unabhängige Cybersicherheitsunternehmen Cure53 hat Audits der Browsererweiterungen und Serversysteme durchgeführt.

Q8: Wie schützt Surfshark vor IPv6-Lecks?

Surfshark leitet IPv6-Verkehr sicher weiter oder schränkt ihn sicher ein, um jedes unverschlüsselte Leck zu verhindern.

Q9: Welcher Rechtsordnung unterliegt Surfshark?

Surfshark unterliegt niederländischem Recht und hält sich an die strengen europäischen Datenschutzstandards der DSGVO (GDPR).

Q10: Unterstützt Surfshark Zwei-Faktor-Authentifizierung (2FA)?

Ja, und Surfshark One fügt eine 2FA-Sperre hinzu, damit nur Sie die Funktionseinstellungen ändern können.

Teil 11: 10 Fakten und Einblicke zu VPNs aus der Praxis

Lernen Sie reale Fakten zu VPN-Verschlüsselungsgeschwindigkeiten, Protokoll-Audits, mobiler Konnektivität und Remote-Arbeit in Unternehmen kennen.

1. VPN-EINBLICK

1. Laut Surfshark läuft sein gesamtes Netzwerk aus über 4.500 Servern auf festplattenloser, flüchtiger reiner RAM-Hardware.

2. VPN-EINBLICK

2. Das Big-Four-Unternehmen Deloitte hat die No-Logs-Richtlinie von Surfshark 2023 und erneut im November 2025 überprüft.

3. VPN-EINBLICK

3. Die proprietäre Nexus-Architektur verbindet alle Server weltweit zu einem dynamischen softwaredefinierten Netzwerk.

4. VPN-EINBLICK

4. Rotating IP ändert Ihre IP-Adresse etwa alle fünf Minuten, ohne die VPN-Verbindung zu trennen.

5. VPN-EINBLICK

5. CleanWeb 2.0 blockiert aufdringliche Cookie-Einwilligungs-Pop-ups und Videowerbung direkt im Browser.

6. VPN-EINBLICK

6. Mit Dynamic MultiHop können Nutzer individuelle Verschlüsselungspfade über zwei Server in 100 Ländern erstellen.

7. VPN-EINBLICK

7. Der Camouflage-Modus entfernt VPN-Header-Signaturen, sodass der Datenverkehr nicht von normalem HTTPS zu unterscheiden ist.

8. VPN-EINBLICK

8. Alternative ID erzeugt Einweg-Pseudonyme und E-Mail-Masken, um Nutzer vor Datenbanklecks zu schützen.

9. VPN-EINBLICK

9. Surfshark setzt bei WireGuard-Protokollen symmetrische AES-256-GCM-Verschlüsselung neben ChaCha20 ein.

10. VPN-EINBLICK

10. Der NoBorders-Modus wird in eingeschränkten Netzwerken automatisch aktiviert, um einen widerstandsfähigen Tunnelzugang zu bieten.

Technische Referenzen und Quellen

Der Lernleitfaden und die interaktiven Rätsel wurden aus globalen technischen Standards, Spezifikationen und Regulierungsrahmen zusammengestellt.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[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

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 **Integrierter Inhaltsblocker** SCHUTZ VOR WERBUNG UND MALWARE — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

CleanWeb ist der integrierte Sicherheitsfilter von Surfshark, der Werbung, Tracker-Domains, Phishing-Websites und bösartige URL-Skripte auf Netzwerkebene blockiert. Quelle: CleanWeb Security Specs.

2 **100 % reine RAM-Infrastruktur** RAM-ARCHITEKTUR — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Surfshark betreibt reine RAM-Server, sodass im Serverspeicher gehaltene Daten gelöscht werden, wenn ein Server ausgeschaltet oder neu gestartet wird. Quelle: Cure53 Infrastructure Audit.

3 **MultiHop-Doppeltunnel** MULTI-HOP-VPN — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

MultiHop (Double VPN) verschlüsselt den Datenverkehr über zwei verschiedene Serverknoten in unterschiedlichen Ländern, um Korrelationsangriffe auf den Datenverkehr zu verhindern. Quelle: Surfshark MultiHop Guide.

4 **Verschleierung mit dem Camouflage-Modus** VERSCHLEIERUNG — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Der Camouflage-Modus verändert die Header von OpenVPN-Paketen, um VPN-Datenverkehr als gewöhnlichen HTTPS-Datenverkehr zu tarnen und so restriktive Firewall-Sperren zu umgehen. Quelle: Surfshark Stealth Whitepaper.

5 **Bypasser-Split-Tunneling** SPLIT TUNNELING — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Bypasser ist das Split-Tunneling-Werkzeug von Surfshark, mit dem Nutzer bestimmte Apps oder Websites auswählen können, die direkt über ihre normale Verbindung des Internetanbieters geleitet werden. Quelle: Surfshark Client Features.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Löschen der Daten im flüchtigen Speicher**

SERVERSICHERHEIT

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Reine RAM-Server speichern keinerlei Daten auf dauerhaften Festplatten; ein Neustart der Hardware leert sofort den gesamten Arbeitsspeicher. Quelle: RAM Server Architecture.

7 **Verbergen vor dem ISP mit dem Camouflage-Modus**

VERSCHLEIERUNG DES DATENVERKEHRS

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Der Camouflage-Modus entfernt die Signaturen des OpenVPN-Protokolls und verhindert so, dass ISPs erkennen, dass der Nutzer mit einem VPN-Tunnel verbunden ist. Quelle: Deep Packet Inspection Guide.

8 **Browsererweiterungen von CleanWeb 2.0**

BROWSERERWEITERUNG

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

CleanWeb 2.0 arbeitet in Browsererweiterungen und blockiert Cookie-Einwilligungs-Pop-ups, Videowerbung und bösartige Weiterleitungsskripte in Echtzeit. Quelle: CleanWeb 2.0 Release Notes.

9 **Keine Speicherung von Verbindungsprotokollen**

NO-LOGS-RICHTLINIE

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Surfshark verfolgt eine strikte, unabhängig geprüfte No-Logs-Richtlinie und zeichnet keine IP-Adressen, Zeitstempel von Verbindungen oder Bandbreitenprotokolle auf. Quelle: Deloitte No-Logs Audit.

10 **Dynamische IP-Rotation mit Nexus**

NEXUS-NETZWERK

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Das softwaredefinierte Netzwerk Surfshark Nexus wechselt die IP-Adressen der Nutzer dynamisch alle paar Minuten, ohne die aktive VPN-Verbindung zu trennen. Quelle: Surfshark Nexus Architecture.

Vokabelschlüssel und Bewertungsraster

Bewertungsraster für Lehrkräfte: Vergeben Sie 1 Punkt für jede richtige Zuordnung (insgesamt 8 Punkte) und jeden Kontextbegriff (insgesamt 6 Punkte).

KONTROLLPUNKT 4: LÖSUNG BEGRIFFSZUORDNUNG

C 1. CLEANWEB	D 2. RAM-SERVER	G 3. MULTI-HOP	F 4. TARNUNG
B 5. UMGEHER	A 6. KILL SWITCH	H 7. NEXUS-NETZWERK	E 8. ROTIEREND

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

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

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

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

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden CLEANWEB, RAM-SERVER und MULTI-HOP in eigenen Worten erklären und jeweils ein Beispiel nennen können.

Fallstudien:
Bitten Sie die Lernenden, ihre Empfehlungen mit Fakten aus dem Arbeitsblatt statt mit Vermutungen zu begründen.

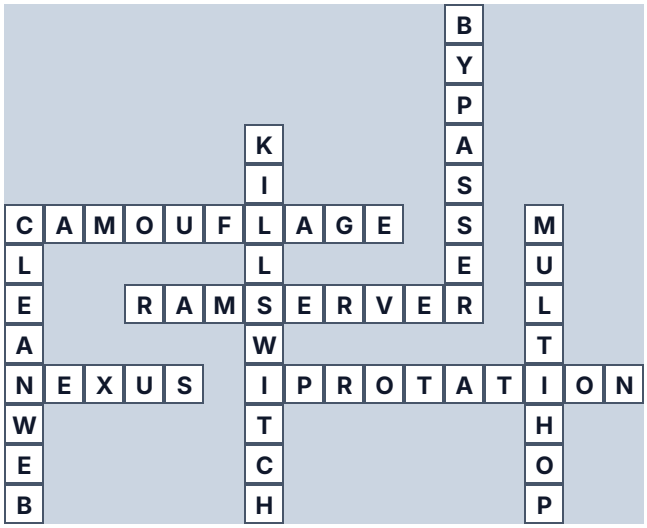
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

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

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

3 waagerecht: CAMOUFLAGE Verschleierungstechnik, die VPN-Signaturen verbirgt, damit der Verkehr wie normales HTTPS aussieht (10 Buchstaben)

5 waagerecht: RAMSERVER Server-Hardware mit flüchtigem Speicher, die bei jedem Stromzyklus alle Daten löscht (9 Buchstaben)

6 waagerecht: NEXUS Proprietäres softwaredefiniertes Netzwerk, das alle Server zu einem einheitlichen Mesh verbindet (5 Buchstaben)

7 waagerecht: IPROTATION Funktion, die Ihre externe IP-Adresse regelmäßig ändert, ohne Tunnel zu unterbrechen (10 Buchstaben)

SENKRECHT

1 senkrecht: BYPASSER Split-Tunneling-Funktion, mit der ausgewählte Anwendungen das VPN umgehen (8 Buchstaben)

2 senkrecht: KILLSWITCH Automatische Sicherheitsfunktion, die den Netzwerkverkehr blockiert, wenn das VPN ausfällt (10 Buchstaben)

3 senkrecht: CLEANWEB Fortschrittlicher Filter, der Werbung, Malware und Cookie-Banner blockiert (8 Buchstaben)

4 senkrecht: MULTIHOP Double-VPN-Funktion, die den Datenverkehr über zwei verschiedene Serverknoten verschlüsselt (8 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

Lösungsschlüssel für die Wort-Entwirr-Aufgabe und die Geheime Chiffre-Aufgabe.

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. E A N C W L B E — **CLEANWEB**
2. T M P U O H I L — **MULTIHOP**
3. A Y B S S R E P — **BYPASSER**
4. X S U N E — **NEXUS**
5. V E A R R S R E M — **RAMSERVER**
6. G U O L A C A F E M — **CAMOUFLAGE**
7. I L K I W T C H S L — **KILLSWITCH**
8. O O A N I T P T I R — **IPROTATION**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"NEXUS IP ROTATION STAERKT DIE PRIVATSPHAERE"

Lösungsschlüssel zu den Fallstudien

A FALLSTUDIE 1: UMGEHUNG VON FILTERN AN HOCHSCHULE UND ARBEITSPLATZ

Lösung für Lehrkräfte

BEWERTUNGSRASTER UND LÖSUNGSHINWEISE

- Szenarioanalyse: Eine Studentin stellt fest, dass das WLAN auf ihrem Universitätscampus alle Standardports von OpenVPN und WireGuard sperrt.
- Leitfrage: Mit welcher Surfshark-Funktion kann sich der Student verbinden, ohne von Netzwerkadministratoren entdeckt zu werden?
- Empfohlene Strategie und Lösung: Aktivieren Sie den Camouflage-Modus (OpenVPN), der VPN-Metadaten verbirgt, sodass Firewalls normales HTTPS-Surfen sehen.

B FALLSTUDIE 2: JOURNALISTISCHE RECHERCHE MIT HOHEM RISIKO

Lösung für Lehrkräfte

BEWERTUNGSRASTER UND LÖSUNGSHINWEISE

- Szenarioanalyse: Eine investigative Journalistin benötigt zusätzlichen Schutz vor Überwachung, während sie zu sensiblen Unternehmensunterlagen recherchiert.
- Leitfrage: Inwiefern bietet Dynamic MultiHop mehr Privatsphäre als das Routing über einen einzelnen Server?
- Empfohlene Strategie und Lösung: Dynamic MultiHop leitet den Traffic über Eingangs- und Ausgangsserver in zwei Ländern, sodass kein einzelner Server den Nutzer offenlegen kann.