Name: _____ Datum: _____ Punkte: _____

Sicherheit von ProtonVPN

Analyse der Sicherheitsarchitektur von ProtonVPN, einschließlich Secure-Core-Servern, NetShield-DNS-Filterung, Schweizer Datenschutz-Rechtsordnung, quelloffener geprüfter Apps und des Stealth-Protokolls.

LERNÜBERSICHT SICHERHEIT VON PROTONVPN

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 Proton VPN und seine Sicherheitsarchitektur. Sie befassen sich mit Secure-Core-Servern mit doppeltem Hop, der DNS-Sperre NetShield, Schweizer Datenschutzgesetzen und der Stealth-Verschleierung.

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/protonvpn/sicherheit/

Ihr Lernfahrplan: ProtonVPN-Sicherheit

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

ANLEITUNG ZUM LEITFADEN SICHERHEIT VON PROTONVPN

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: Secure-Core-Double-Hop-Routing und Schweizer Datenschutzregeln. Zum Schluss folgt die Bonusaufgabe Schnell denken.

SECURE-CORE-DOUBLE-HOP-ARCHITEKTUR UND SCHWEIZER DATENSCHUTZRECHT

Proton VPN schützt den Datenverkehr der Nutzer mit eigenen Secure-Core-Servern in der Schweiz, Island und Schweden, quelloffenen, geprüften Apps und dem Verschleierungsprotokoll Stealth, das die Deep Packet Inspection umgehen soll.

(EINFÜHRUNG)

Proton VPN schützt den Datenverkehr der Nutzer mit eigenen Secure-Core-Servern in der Schweiz, Island und Schweden, quelloffenen, geprüften Apps und dem Verschleierungsprotokoll Stealth, das die Deep Packet Inspection umgehen soll.

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

Kontrollpunkt 1: Auswahlaufgaben

1. In welchen Einrichtungen stehen die Secure-Core-Server von Proton?

- A) Öffentliche Cloud-VMs
- B) Hochsicherheitsstandorte
- C) Öffentliche Rechenzentren
- D) Gemeinsam genutzte Racks

2. Welches Protokoll hilft, strenge staatliche Zensur zu umgehen?

- A) PPTP
- B) Stealth-Protokoll
- C) OpenVPN UDP
- D) IKEv2

3. Welche Funktion hat NetShield von Proton VPN?

- A) Speed Booster
- B) DNS-Werbe- und Malware-Blocker
- C) Cloud-Speicher
- D) Portweiterleitung

4. Unter den Datenschutzgesetzen welches Landes ist die Proton AG tätig?

- A) Vereinigte Staaten
- B) Vereinigtes Königreich
- C) Schweiz
- D) Panama

5. Wie werden die Client-Apps von Proton VPN durch Fachleute überprüft?

- A) Geheimcode
- B) Open-Source-Audits
- C) Proprietäre Lizenz
- D) Behördliche Prüfung

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Secure Core leitet den Datenverkehr vor dem Austritt über datenschutzfreundliche Länder.

○ Richtig ○ Falsch

7 Frage 7

7. Die Schweiz ist Mitglied der Geheimdienst-Überwachungsallianz der 14 Eyes.

○ Richtig ○ Falsch

8 Frage 8

8. NetShield blockiert Werbung und schädliche Domains direkt auf DNS-Ebene.

○ Richtig ○ Falsch

9 Frage 9

9. Die Apps von Proton VPN sind zu 100% quelloffen und öffentlich geprüft.

○ Richtig ○ Falsch

10 Frage 10

10. Das Stealth-Protokoll verwendet standardmäßige WireGuard-Header ohne Verschleierung.

○ 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. Multi-Hop-Routing über Proton-eigene Server in datenschutzfreundlichen Ländern nennt man die Architektur _____ .

2. Um Deep Packet Inspection und Netzwerk-Firewalls auszuhebeln, aktivieren Nutzer den Modus _____ .

3. Malware-Domains, Tracker und Werbeskripte werden per DNS durch _____ gefiltert.

4. Laut Proton ist das Unternehmen nach _____ nicht verpflichtet, Protokolle über Nutzeraktivitäten zu führen.

5. Bricht der VPN-Tunnel unerwartet ab, blockiert der _____ den Internetverkehr.

6. Unabhängige Sicherheitsforscher können die Integrität der Clients prüfen, weil die Apps _____ sind.

WORTSCHATZ-WORTBANK

AES-GCM KILL SWITCH NETSHIELD OPEN SOURCE SCHWEIZER RECHT
SECURE CORE STEALTH WIREGUARD

Schreiben Sie Ihre Antworten hier:

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

Kontrollpunkt 4: Zuordnung von VPN- und Netzwerk-Begriffen

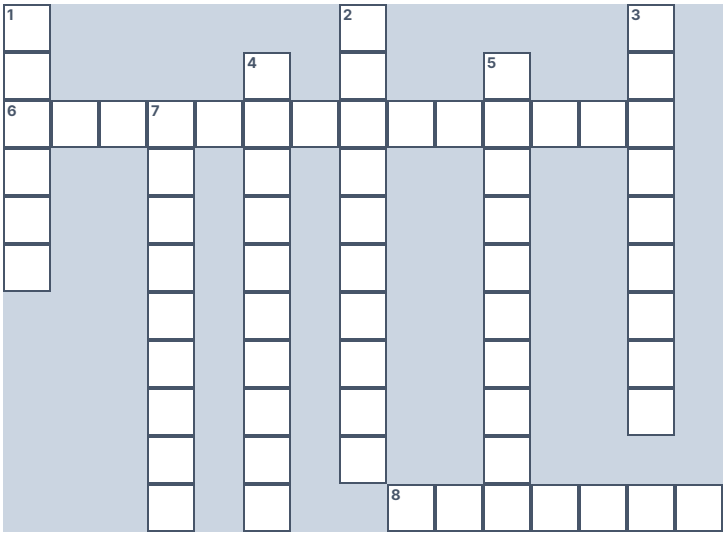
DEFINITIONEN ZUORDNEN

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

☐	1. SECURE CORE	A	Öffentlich zugängliche und unabhängig geprüfte Client-Software.
☐	2. STEALTH-PROTOKOLL	B	Standard für symmetrische Chiffren, der die Datenpakete des VPN verschlüsselt.
☐	3. NETSHIELD	C	Strenge gesetzliche Datenschutzbestimmungen in der Schweiz, außerhalb der Rechtsordnungen der 14 Eyes.
☐	4. SCHWEIZER GESETZE	D	Ein verschleiertes Tunnelprotokoll, getarnt als normaler HTTPS-Webverkehr.
☐	5. KILL SWITCH	E	Ein modernes, schlankes Protokoll mit robuster Kryptografie und hohen Geschwindigkeiten.
☐	6. OPEN SOURCE	F	Ein DNS-basierter Filter, der Werbung, Telemetrie-Tracker und Malware blockiert.
☐	7. WIREGUARD	G	Ein Multi-Hop-Design, das den Datenverkehr über Proton-eigene Server als ersten Hop leitet.
☐	8. AES256-GCM	H	Eine Schutzmaßnahme, die die Netzwerkübertragung bei Verbindungsabbrüchen stoppt.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

6. Strenge gesetzliche Datenschutzvorschriften in der Schweiz, außerhalb des 14-Eyes-Rechtsraums (14)

8. Verschleiertes Tunnelprotokoll, das als normaler HTTPS-Webverkehr getarnt ist (7)

SENKRECHT

1. Symmetrische Chiffre auf Militärniveau, die alle gekapselten VPN-Datenpakete sichert (6)

2. Öffentlich zugängliche und unabhängig geprüfte Client-Software (10)

3. DNS-basierter Filter, der Werbung, Telemetrie-Tracker und Malware blockiert (9)

4. Sicherheitsvorkehrung, die die Netzwerkübertragung bei Verbindungsabbrüchen stoppt (10)

5. Multi-Hop-Design, das den Datenverkehr über Proton-eigene Server als ersten Hop leitet (10)

7. Modernes, schlankes Protokoll mit robuster Kryptografie und hoher Geschwindigkeit (9)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

6 waagerecht: Strenge gesetzliche Datenschutzvorschriften in der Schweiz, außerhalb des 14-Eyes-Rechtsraums (14 Buchstaben):

8 waagerecht: Verschleiertes Tunnelprotokoll, das als normaler HTTPS-Webverkehr getarnt ist (7 Buchstaben):

SENKRECHT

1 senkrecht: Symmetrische Chiffre auf Militärniveau, die alle gekapselten VPN-Datenpakete sichert (6 Buchstaben):

2 senkrecht: Öffentlich zugängliche und unabhängig geprüfte Client-Software (10 Buchstaben):

3 senkrecht: DNS-basierter Filter, der Werbung, Telemetrie-Tracker und Malware blockiert (9 Buchstaben):

4 senkrecht: Sicherheitsvorkehrung, die die Netzwerkübertragung bei Verbindungsabbrüchen stoppt (10 Buchstaben):

5 senkrecht: Multi-Hop-Design, das den Datenverkehr über Proton-eigene Server als ersten Hop leitet (10 Buchstaben):

7 senkrecht: Modernes, schlankes Protokoll mit robuster Kryptografie und hoher Geschwindigkeit (9 Buchstaben):

Kontrollpunkt 6: Suchsel

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

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

WORTSCHATZ-WORTLISTE

SECURECORE STEALTH NETSHIELD SCHWEIZERRECHT KILLSWITCH
OPENSOURCE WIREGUARD AESGCM

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. SECURECORE**
- **B. STEALTH**
- **C. NETSHIELD**
- **D. SCHWEIZERRECHT**
- **E. KILLSWITCH**
- **F. OPENSOURCE**
- **G. WIREGUARD**
- **H. AESGCM**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Verschleiertes Tunnelprotokoll, das als normaler HTTPS-Webverkehr getarnt ist.

_____ 2. Modernes, schlankes Protokoll mit robuster Kryptografie und hoher Geschwindigkeit.

_____ 3. Strenge gesetzliche Datenschutzvorschriften in der Schweiz, außerhalb des 14-Eyes-Rechtsraums.

_____ 4. Multi-Hop-Design, das den Datenverkehr über Proton-eigene Server als ersten Hop leitet.

_____ 5. Symmetrische Chiffre auf Militärniveau, die alle gekapselten VPN-Datenpakete sichert.

_____ 6. Sicherheitsvorkehrung, die die Netzwerkübertragung bei Verbindungsabbrüchen stoppt.

_____ 7. DNS-basierter Filter, der Werbung, Telemetrie-Tracker und Malware blockiert.

_____ 8. Öffentlich zugängliche und unabhängig geprüfte Client-Software.

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. RCERESOEUC
2. DNLSEIEHT
3. KWCIISHLTL
4. GDREAUWIR
5. LHAESTT
6. IZEEHCEHRSCRTW
7. PNOUORCESE
8. SMACGE

Bonusaufgabe: Schnell denken

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

1	Dinge, die Sie jeden Tag online tun			
2	Länder, die für strenge Datenschutzgesetze bekannt sind			
3	Sicherheitsfunktionen von Proton VPN			
4	Arten von VPN-Lecks			
5	Situationen, in denen ein Kill Switch hilft			
6	Dinge, die ein Audit prüfen kann			
7	Einstellungen, die Sie für mehr Sicherheit einschalten			
8	Dinge, die Verschlüsselung schützt			
9	Wörter, die eine gute VPN-App beschreiben			
10	Gründe, sich für Proton VPN zu entscheiden			
11	Schaltflächen oder Menüs in einer VPN-App			
12	Streamingdienste, die Sie nutzen			
13	Bedrohungen in öffentlichen WLANs			
14	Möglichkeiten, ein starkes Passwort zu erstellen			
15	Länder, in denen Sie Server von Proton VPN haben möchten			

Kontrollpunkt 8: Fallstudien zu VPN und Netzwerken

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

FALLSTUDIE 1: UMGEHUNG RESTRIKTIVER FIREWALLS



Szenario: Ein Nutzer reist in ein Land, in dem gängiger VPN-Verkehr wie OpenVPN und WireGuard per DPI blockiert wird.

Diskussionsfrage: Mit welcher Protokollkonfiguration von Proton VPN kann der Nutzer die staatliche Paketprüfung umgehen?

FALLSTUDIE 2: SCHUTZ VOR FORTGESCHRITTENEN ANGREIFERN



Szenario: Ein Finanzprüfer vermutet, dass der Ausgangsknoten seines lokalen Internetanbieters durch fortgeschrittene, andauernde Bedrohungen (APT) kompromittiert sein könnte.

Diskussionsfrage: Wie schützt Secure Core die Identität des Prüfers bei einer Kompromittierung des Ausgangsknotens?

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

19	5	3	21	18	5		3	15	18	5		19	5	18	22	5	18

19	3	8	21	5	20	26	5	14

14	21	20	26	5	18	4	1	20	5	14

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 Proton VPN Secure Core?

Secure Core leitet den Datenverkehr vor dem Austritt über mehrere Server in datenschutzfreundlichen Ländern.

Q2: Was ist das Stealth-Protokoll?

Stealth ist ein verschleiertes Protokoll, das VPN-Verbindungen als normalen TLS/HTTPS-Verkehr tarnt.

Q3: Wie schützt NetShield die Nutzer?

NetShield ist ein DNS-basiertes Werkzeug, das Werbung, Tracker und Malware-Domains automatisch blockiert.

Q4: Ist Proton VPN in der Schweiz rechtlich geschützt?

Ja, die Schweiz hat strenge Datenschutzgesetze und liegt außerhalb des Rechtsraums der USA und der EU/14 Eyes. [4]

Q5: Sind die Apps von Proton VPN Open Source?

Ja. Die Apps von Proton VPN sind Open Source und wurden in veröffentlichten Sicherheitsaudits geprüft.

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: Welche Verschlüsselungschiffren werden verwendet?

Proton VPN nutzt AES-256-GCM oder ChaCha20-Poly1305 mit HMAC-SHA384 und RSA-4096-Handshakes.

Q7: Hat Proton VPN einen Kill Switch?

Ja, Proton VPN enthält einen normalen und einen permanenten Kill Switch, um unverschlüsselte Leaks zu verhindern.

Q8: Kann Proton VPN DNS-Anfragen preisgeben?

Nein, alle DNS-Anfragen werden über verschlüsselte private DNS-Server von Proton geleitet.

Q9: Speichert Proton VPN Verbindungsprotokolle?

Nein, Proton VPN verfolgt eine strikte No-Logs-Richtlinie, die durch jährliche Audits von Securitum bestätigt wird. [3]

Q10: Ist Proton VPN anfällig für WebRTC-Leaks?

Nein, die Proton-Clients enthalten integrierte Firewall-Regeln und Routing-Richtlinien, die WebRTC-Lecks blockieren.

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: Wo befinden sich die Secure-Core-Rechenzentren physisch?

Sie befinden sich in der Schweiz, auf einem ehemaligen Militärstützpunkt in Island und an einem unterirdischen Standort in Schweden. [1]

Q2: Wie funktioniert Perfect Forward Secrecy in Proton VPN?

Für jede Sitzung wird ein eigener, kurzlebiger Schlüssel erzeugt, was eine nachträgliche Entschlüsselung verhindert.

Q3: Was ist der Permanent Kill Switch unter Windows/Linux?

Ein permanenter Kill Switch blockiert sämtlichen Netzwerkverkehr, selbst wenn die VPN-App vollständig geschlossen ist oder abstürzt.

Q4: Unterstützt Proton VPN IPv6-Routing und den Schutz vor Lecks?

Proton VPN leitet IPv6-Verkehr vollständig durch Tunnel oder deaktiviert ihn sicher, um Leaks zu verhindern.

Q5: Wie geht die DNS-Filterung von NetShield mit der HTTPS-Prüfung um?

NetShield arbeitet ausschließlich auf der Ebene der DNS-Auflösung, ohne eine invasive TLS-Entschlüsselung zu benötigen.

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: Wer hat die externen Code-Audits von Proton VPN durchgeführt?

SEC Consult hat die Apps geprüft, und Securitum prüft die Apps sowie die No-Logs-Richtlinie.

Q7: Wie schneidet das Stealth-Protokoll im Vergleich zu OpenVPN XOR oder Shadowsocks ab?

Stealth tunnelt WireGuard über verschleiertes TLS und ist leistungsfähiger als ältere OpenVPN-basierte Verschleierung. [5]

Q8: Können Schweizer Behörden Proton VPN zwingen, Traffic zu protokollieren?

Proton erklärt, dass es nach Schweizer Recht nicht verpflichtet ist, Logs zu Nutzeraktivitäten oder -daten aufzubewahren.

Q9: Wie sind die Server von Proton VPN vor Beschlagnahmung geschützt?

Alle Proton-VPN-Server sind Bare-Metal-Maschinen mit Festplattenvollverschlüsselung. [2]

Q10: Unterstützt Proton VPN die Konfiguration eigener DNS-Server?

Ja, zahlende Abonnenten können eigene Upstream-DNS-Server direkt in den App-Einstellungen konfigurieren.

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. Proton besitzt seine Secure-Core-Server selbst und installiert sie in Hochsicherheitsstandorten in der Schweiz, in Island und in Schweden. [1]

2. VPN-EINBLICK

2. Die Client-Apps von Proton VPN sind quelloffen und werden regelmäßig Code-Audits durch Dritte unterzogen.

3. VPN-EINBLICK

3. Das Verschleierungsprotokoll Stealth umgeht die Deep Packet Inspection, indem es normalen TLS-Verkehr simuliert.

4. VPN-EINBLICK

4. Die Schweiz gehört nicht zu den internationalen Geheimdienstallianzen 5-Eyes, 9-Eyes und 14-Eyes. [4]

5. VPN-EINBLICK

5. NetShield arbeitet auf der Ebene des DNS-Resolvers und verhindert Werbung und Malware, bevor die Nutzdaten heruntergeladen werden.

6. VPN-EINBLICK

6. Perfect Forward Secrecy stellt sicher, dass kompromittierte Schlüssel zuvor aufgezeichnete Datenverkehrssitzungen nicht entschlüsseln können. [7]

7. VPN-EINBLICK

7. Proton VPN nutzt Festplattenvollverschlüsselung auf Bare-Metal-Servern, um Serverkonfigurationen zu schützen. [2]

8. VPN-EINBLICK

8. Der permanente Kill Switch verhindert unverschlüsselte Datenlecks selbst bei Neustarts des Betriebssystems.

9. VPN-EINBLICK

9. Securitum hat die No-Logs-Richtlinie von Proton VPN in fünf aufeinanderfolgenden jährlichen Audits geprüft und bestätigt. [3]

10. VPN-EINBLICK

10. Proton VPN wurde von Wissenschaftlern entwickelt, die sich am CERN (Europäische Organisation für Kernforschung) kennengelernt hatten. [4]

Technische Referenzen und Quellen

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

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] Proton VPN. (n.d.). What is Secure Core?
https://protonvpn.com/support/secure-core-vpn

[2] Proton VPN. (n.d.). Proton VPN features.
https://protonvpn.com/features

[3] Proton VPN. (n.d.). Proton VPN passes 5th annual external audit of no-logs policy.
https://protonvpn.com/blog/no-logs-audit

[4] Proton VPN. (n.d.). Get a VPN protected by Swiss privacy laws.
https://protonvpn.com/features/swiss-based

[5] Proton VPN. (2022). Defeat censorship with Stealth, our new VPN protocol.
https://protonvpn.com/blog/stealth-vpn-protocol

[6] GitHub. (n.d.). ProtonVPN · GitHub.
https://github.com/ProtonVPN

[7] WireGuard. (n.d.). Protocol & Cryptography.
https://www.wireguard.com/protocol/

[8] IETF. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols.
https://www.rfc-editor.org/rfc/rfc8439

[9] NIST. (2007). SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.
https://csrc.nist.gov/pubs/sp/800/38/d/final

[10] IETF. (2014). RFC 7359: Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks.
https://www.rfc-editor.org/rfc/rfc7359

[11] IETF. (2021). RFC 9076: DNS Privacy Considerations.
https://www.rfc-editor.org/rfc/rfc9076

[12] Federal Data Protection and Information Commissioner. (n.d.). Federal Data Protection and Information Commissioner (FDPIC).
https://www.edoeb.admin.ch/en

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 **Frage 1** — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Secure-Core-Server stehen an Hochsicherheitsstandorten, darunter ein ehemaliger Militärstützpunkt in Island und ein unterirdisches Rechenzentrum in Schweden.

2 **Stealth-Verschleierungsprotokoll** ABWEHR VON ZENSUR — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Das Stealth-Protokoll von Proton tarnt WireGuard-Verbindungen als normalen TLS/HTTPS-Verkehr, um Firewalls mit Deep Packet Inspection (DPI) zu umgehen. Quelle: Proton Stealth Protocol Whitepaper.

3 **NetShield-DNS-Werbeblocker** DNS-FILTERUNG — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

NetShield nutzt Filterung auf DNS-Ebene, um Malware-Domains, Spyware, aufdringliche Werbung und Telemetrie-Tracker zu blockieren, bevor Webseiten geladen werden. Quelle: NetShield Security Specs.

4 **Schweizer Rechtsordnung** GERICHTSBARKEIT — **Richtige Antwort: C**

HINWEIS FÜR LEHRKRÄFTE

Proton AG hat seinen Hauptsitz in Genf, Schweiz, und profitiert von strengen Schweizer Datenschutzgesetzen außerhalb der Überwachungsallianzen der USA und der EU (14 Eyes). Quelle: Swiss Federal Data Protection Act.

5 **Frage 5** — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Alle Proton-VPN-Apps sind Open Source; SEC Consult und später Securitum haben sie geprüft.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Secure Core über mehrere Rechtsordnungen** ROUTING-ARCHITEKTUR **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Secure Core leitet den Datenverkehr über Rechtsordnungen mit besonders starkem Datenschutz, bevor er im Zielland austritt, und hilft so beim Schutz vor einem kompromittierten Ausgangsserver. Quelle: Secure Core Architecture.

7 **Schweizer Überwachungsallianz** ÜBERWACHUNGSALLIANZEN **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Die Schweiz ist nicht Mitglied der Geheimdienstabkommen der 5 Eyes, 9 Eyes oder 14 Eyes und wahrt so ihre unabhängige rechtliche Souveränität. Quelle: International Surveillance Treaties.

8 **Frage 8** **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

NetShield nutzt die DNS-Server von Proton, um Domains mit Listen bekannter Werbe-, Tracker- und Malware-Domains abzugleichen.

9 **Prüfung von Open-Source-Clients** SICHERHEITSTRANSPARENZ **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Proton hat seine Desktop- und Mobil-Apps als Open Source veröffentlicht und publiziert Prüfberichte von Dritten. Quelle: SEC Consult Security Report.

10 **Frage 10** **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Falsch: Stealth tunnelt WireGuard in verschleiertem TLS über TCP, sodass der Datenverkehr wie gewöhnliches HTTPS aussieht.

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

G 1. SECURE CORE	D 2. STEALTH-PROTOKOLL	F 3. NETSHIELD	C 4. SCHWEIZER GESETZE
H 5. KILL SWITCH	A 6. OPEN SOURCE	E 7. WIREGUARD	B 8. AES256-GCM

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 SECURE CORE	2 STEALTH	3 NETSHIELD	4 SCHWEIZER RECHT
5 KILL SWITCH	6 OPEN SOURCE		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 B – STEALTH	2 G – WIREGUARD	3 D – SCHWEIZERRECHT	4 A – SECURECORE
5 H – AESGCM	6 E – KILLSWITCH	7 C – NETSHIELD	8 F – OPENSOURCE

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden SECURE CORE, STEALTH-PROTOKOLL und NETSHIELD 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

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

KREUZWORTRÄTSEL-LÖSUNG

A						O						N
E				K		P			S			E
S	C	H	W	E	I	E	R	R	E	C	H	T
G			I		L	N			C			S
C			R		L	S			U			H
M			E		S	O			R			I
			G		W	U			E			E
			U		I	R			C			L
			A		T	C			O			D
			R		C	E			R			
			D		H		S	T	E	A	L	T	H

LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

6 waagerecht: SCHWEIZERRECHT Strenge gesetzliche Datenschutzvorschriften in der Schweiz, außerhalb des 14-Eyes-Rechtsraums (14 Buchstaben)

8 waagerecht: STEALTH Verschleiertes Tunnelprotokoll, das als normaler HTTPS-Webverkehr getarnt ist (7 Buchstaben)

SENKRECHT

1 senkrecht: AESGCM Symmetrische Chiffre auf Militärniveau, die alle gekapselten VPN-Datenpakete sichert (6 Buchstaben)

2 senkrecht: OPENSOURCE Öffentlich zugängliche und unabhängig geprüfte Client-Software (10 Buchstaben)

3 senkrecht: NETSHIELD DNS-basierter Filter, der Werbung, Telemetrie-Tracker und Malware blockiert (9 Buchstaben)

4 senkrecht: KILLSWITCH Sicherheitsvorkehrung, die die Netzwerkübertragung bei Verbindungsabbrüchen stoppt (10 Buchstaben)

5 senkrecht: SECURECORE Multi-Hop-Design, das den Datenverkehr über Proton-eigene Server als ersten Hop leitet (10 Buchstaben)

7 senkrecht: WIREGUARD Modernes, schlankes Protokoll mit robuster Kryptografie und hoher Geschwindigkeit (9 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. RCERESOEUC — SECURECORE
2. DNLSEIEHT — NETSHIELD
3. KWCIISHLTL — KILLSWITCH
4. GDREAUWIR — WIREGUARD
5. LHAESTT — STEALTH
6. IZEEHCEHRSCRTW — SCHWEIZERRECHT
7. PNOUORCESE — OPENSOURCE
8. SMACGE — AESGCM

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"SECURE CORE SERVER SCHUETZEN NUTZERDATEN"

Lösungsschlüssel zu den Fallstudien

A FALLSTUDIE 1: UMGEHUNG RESTRIKTIVER FIREWALLS

Lösung für Lehrkräfte

BEWERTUNGSRASTER UND LÖSUNGSHINWEISE

- Szenarioanalyse: Ein Nutzer reist in ein Land, in dem normaler VPN-Verkehr wie OpenVPN und WireGuard per DPI blockiert wird.
- Leitfrage: Mit welcher Protokollkonfiguration von Proton VPN kann der Nutzer staatliche Inspektion umgehen?
- Empfohlene Strategie und Lösung: Der Nutzer sollte das Stealth-Protokoll aktivieren, das die Header der VPN-Pakete als regulären TLS/HTTPS-Webverkehr tarnt und so an DPI-Filtern vorbeikommt.

B FALLSTUDIE 2: SCHUTZ VOR FORTGESCHRITTENEN ANGREIFERN

Lösung für Lehrkräfte

BEWERTUNGSRASTER UND LÖSUNGSHINWEISE

- Szenarioanalyse: Ein Finanzprüfer vermutet, dass der Ausgangsknoten seines lokalen ISP durch fortgeschrittene, andauernde Bedrohungen (APTs) kompromittiert sein könnte.
- Leitfrage: Wie schützt Secure Core die Identität des Prüfers, falls ein Exit-Knoten kompromittiert wird?
- Empfohlene Strategie und Lösung: Secure Core leitet den Datenverkehr zunächst über Proton-eigene Server in der Schweiz, in Island oder Schweden, sodass ein kompromittierter Ausgangsserver die IP des Nutzers nicht zurückverfolgen kann.