Name: _____ Datum: _____ Punkte: _____

Test von IPVanish

Technische Analyse von IPVanish VPN mit Hauptsitz in den USA: größtenteils eigene Server

LERNÜBERSICHT: TEST VON IPVANISH

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 den technischen Überblick über IPVanish. Sie lernen die physische Infrastruktur im Eigenbesitz, SOCKS5-Proxys für P2P-Torrenting, die WireGuard-Leistung und US-amerikanische Datenvorschriften 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/ipvanish/

Ihr Lernfahrplan: IPVanish

- Analysieren Sie die technische Architektur und die Verschlüsselungsstandards im Testbericht zu IPVanish.
- Konfigurieren Sie die Client-Einstellungen so, dass IP-, DNS- und WebRTC-Leaks verhindert werden.
- Vergleichen Sie proprietäre Tunnelprotokolle mit Standardimplementierungen.

ANLEITUNG: TEST VON IPVANISH

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: SOCKS5-Proxys und eigene Serverinfrastruktur. Zum Schluss folgt die Bonusaufgabe Schnell denken.

EIGENE INFRASTRUKTUR UND SOCKS5-P2P-PROXYS (EINFÜHRUNG)

IPVanish hebt sich dadurch ab, dass es einen großen Teil seines physischen Servernetzes selbst besitzt und verwaltet, was Leistung und Sicherheit verbessert. Es bietet das schnelle WireGuard-Protokoll und SOCKS5-Proxys für P2P-Torrenting, unterliegt aber der US-Gerichtsbarkeit innerhalb der Five Eyes.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Welches Open-Source-Protokoll ist in den Client-Apps von IPVanish standardmäßig für hohe Geschwindigkeit eingestellt?

- A) WireGuard
- B) L2TP/IPSec
- C) PPTP
- D) Catapult Hydra

2. Welche Art von Proxy-Server stellt IPVanish zur Unterstützung von P2P-Torrenting bereit?

- A) SOCKS5-Proxy
- B) HTTP-Proxy
- C) Tor-Relay
- D) Shadowsocks

3. Welches Unternehmen führte 2022 das erste unabhängige No-Logs-Audit von IPVanish durch?

- A) Leviathan Security Group
- B) PwC
- C) Deloitte
- D) Cure53

4. Unter welcher nationalen Gerichtsbarkeit sind die Unternehmensgesellschaften von IPVanish hauptsächlich tätig?

- A) Vereinigte Staaten
- B) Schweiz
- C) Panama
- D) Britische Jungferninseln

5. Wie viele gleichzeitige Geräteverbindungen erlaubt ein Premium-Tarif von IPVanish?

- A) Unbegrenzt
- B) Fünf
- C) Zehn
- D) Sieben

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. IPVanish verwaltet und besitzt einen großen Teil seiner physischen Serverinfrastruktur.

○ Richtig ○ Falsch

7 Frage 7

7. Der Verkehr über SOCKS5-Proxys ist bei der Übertragung genauso vollständig verschlüsselt wie bei normalen VPN-Tunneln.

○ Richtig ○ Falsch

8 Frage 8

8. Dem Desktop-Client von IPVanish fehlt eine Kill-Switch-Funktion auf Systemebene.

○ Richtig ○ Falsch

9 Frage 9

9. IPVanish operiert aus den Vereinigten Staaten, einem Mitglied der Five-Eyes-Geheimdienstallianz.

○ Richtig ○ Falsch

10 Frage 10

10. Split Tunneling in IPVanish ermöglicht es, App-Verkehr außerhalb des VPN-Tunnels zu leiten.

○ 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. Das moderne Protokoll _____ ist standardmäßig für eine optimierte Routing-Leistung konfiguriert.

2. P2P-Datenverkehr kann über einen schnellen _____ geleitet werden, um die echten Standorte der Clients zu verschleiern.

3. Die Verbindung zu einem geografisch nahen Knoten maximiert die tatsächliche _____ .

4. Um Datenlecks zu verhindern, sollten Nutzer den integrierten _____ konfigurieren.

5. Ein _____ durch unabhängige Sicherheitsfirmen hat die Zusage des Anbieters zertifiziert.

6. Anders als manche Konkurrenten setzt IPVanish bei Konten kein aktives _____ .

WORTSCHATZ-WORTBANK

GERÄTELIMIT IP-ADRESSE KILL SWITCH NO-LOGS-AUDIT SERVERLEISTUNG SICHERHEIT SOCKS5-PROXY WIREGUARD

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von VPN- und Netzwerk-Begriffen

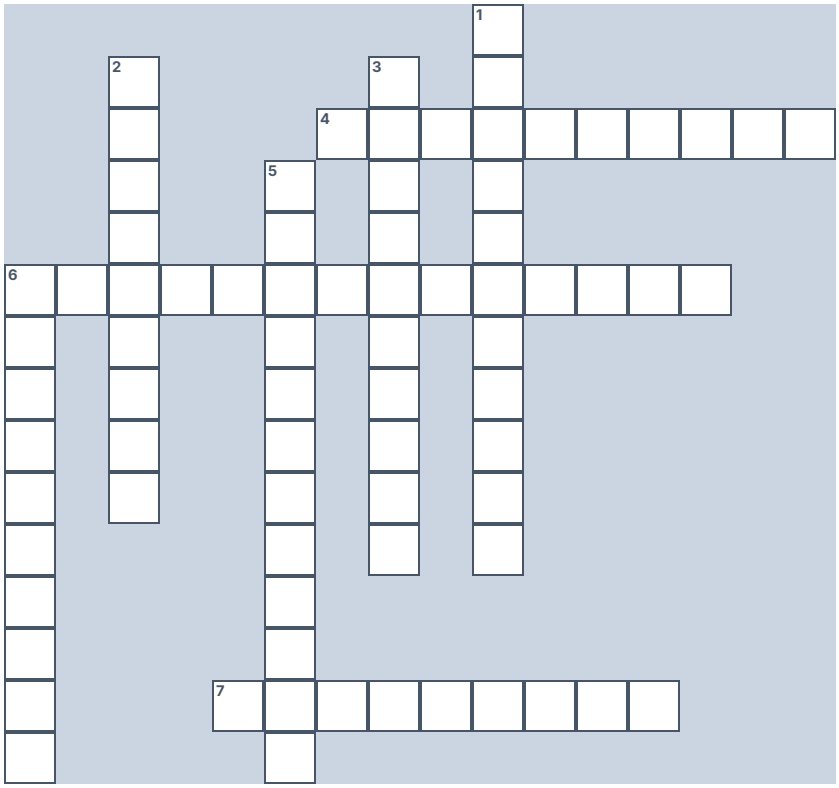
DEFINITIONEN ZUORDNEN

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

☐	1. WireGuard	A	Ausfallsicherung, die den Internetverkehr blockiert, wenn das VPN ausfällt.
☐	2. SOCKS5-Proxy	B	Quelloffenes Protokoll, bekannt für Geschwindigkeit und moderne Kryptografie.
☐	3. Servergeschwindigkeit	C	Einschränkung, die die Anzahl aktiver Gerätesitzungen begrenzt.
☐	4. Kill Switch	D	Durchsatzkapazität eines Serverknotens unter aktiver Verkehrslast.
☐	5. Geprüfte Protokolle	E	Eindeutige Netzwerkkennung, die Geräten im Internet zugewiesen wird.
☐	6. Gerätelimit	F	Gesamter Schutzstatus des verschlüsselten Tunnelsystems.
☐	7. IP-Adresse	G	Geprüfte Nachweise, die bestätigen, dass keinerlei Nutzeraktivität verfolgt wird.
☐	8. Sicherheit	H	Unverschlüsseltes Proxy-Routing-System, mit dem der Standort von P2P-Clients verborgen wird.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

4. Ausfallsicherung, die den Internetverkehr blockiert, wenn das VPN ausfällt (10)

6. Durchsatzkapazität eines Serverknotens unter aktiver Last (14)

7. Open-Source-Protokoll, bekannt für Geschwindigkeit und moderne Kryptografie (9)

SENKRECHT

1. Geprüfte Nachweise, die bestätigen, dass keinerlei Nutzeraktivität erfasst wird (11)

2. Eindeutige Netzwerkkennung, die Geräten im Internet zugewiesen wird (9)

3. Gesamtes Schutzniveau des verschlüsselten Tunnelsystems (10)

5. Beschränkung der Anzahl aktiver Gerätesitzungen (12)

6. Unverschlüsseltes Proxy-System (SOCKS5), mit dem die Standorte von P2P-Clients verschleiert werden (10)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

4 waagerecht: Ausfallsicherung, die den Internetverkehr blockiert, wenn das VPN ausfällt (10 Buchstaben):

6 waagerecht: Durchsatzkapazität eines Serverknotens unter aktiver Last (14 Buchstaben):

7 waagerecht: Open-Source-Protokoll, bekannt für Geschwindigkeit und moderne Kryptografie (9 Buchstaben):

SENKRECHT

1 senkrecht: Geprüfte Nachweise, die bestätigen, dass keinerlei Nutzeraktivität erfasst wird (11 Buchstaben):

2 senkrecht: Eindeutige Netzwerkkennung, die Geräten im Internet zugewiesen wird (9 Buchstaben):

3 senkrecht: Gesamtes Schutzniveau des verschlüsselten Tunnelsystems (10 Buchstaben):

5 senkrecht: Beschränkung der Anzahl aktiver Gerätesitzungen (12 Buchstaben):

6 senkrecht: Unverschlüsseltes Proxy-System (SOCKS5), mit dem die Standorte von P2P-Clients verschleiert werden (10 Buchstaben):

Kontrollpunkt 6: Suchsel

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

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

WORTSCHATZ-WORTLISTE

WIREGUARD SOCKSPROXY SERVERLEISTUNG KILLSWITCH NOLOGSAUDIT
GERAETELIMIT IPADRESSE SICHERHEIT

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. WIREGUARD**
- **B. SOCKSPROXY**
- **C. SERVERLEISTUNG**
- **D. KILLSWITCH**
- **E. NOLOGSAUDIT**
- **F. GERAETELIMIT**
- **G. IPADRESSE**
- **H. SICHERHEIT**

DEFINITIONEN UND ZUORDNUNGSFELDER

1. Unverschlüsseltes Proxy-System (SOCKS5), mit dem die Standorte von P2P-Clients verschleiert werden.
2. Gesamtes Schutzniveau des verschlüsselten Tunnelsystems.
3. Beschränkung der Anzahl aktiver Gerätesitzungen.
4. Durchsatzkapazität eines Serverknotens unter aktiver Last.
5. Open-Source-Protokoll, bekannt für Geschwindigkeit und moderne Kryptografie.
6. Eindeutige Netzwerkkennung, die Geräten im Internet zugewiesen wird.
7. Ausfallsicherung, die den Internetverkehr blockiert, wenn das VPN ausfällt.
8. Geprüfte Nachweise, die bestätigen, dass keinerlei Nutzeraktivität erfasst wird.

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. UGEIWARDR
2. EERRLNSUEGSTIV
3. NASULOITGDO
4. RESDSEIPA
5. OPYOKRSSXC
6. CSLITKIWHL
7. LIEGEETMIRTA
8. IHRTSEIHEC

Bonusaufgabe: Schnell denken

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

1	Wörter, die eine gute VPN-App beschreiben			
2	Dinge, die IPVanish vor Ihrem Netzwerk verbergen kann			
3	Orte, an denen Sie IPVanish einschalten würden			
4	VPN-Protokolle, die Sie kennen			
5	Fragen an den Kundensupport von IPVanish			
6	Länder, in denen Sie Server von IPVanish haben möchten			
7	VPN-Dienste außer IPVanish			
8	Situationen, in denen ein Kill Switch hilft			
9	Gründe, sich für IPVanish zu entscheiden			
10	Anzeichen, dass Ihre VPN-Verbindung langsam ist			
11	Dinge, die Sie jeden Tag online tun			
12	Personen, denen Sie IPVanish empfehlen würden			
13	Dinge, die Sie vor dem Kauf eines VPN prüfen sollten			
14	Sicherheitsbegriffe, die Sie in diesem Arbeitsblatt gelernt haben			
15	Funktionen, auf die Sie bei IPVanish achten			

Kontrollpunkt 8: Fallstudien zu VPN und Netzwerken

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

FALLSTUDIE 1: KONFIGURATION EINES MEDIACENTERS



Szenario: Ein Kunde möchte seinen Android-basierten Fire-TV-Mediaplayer mit IPVanish absichern, um sicher zu streamen und dabei einen hohen Durchsatz beizubehalten.

Diskussionsfrage: Warum wird das WireGuard-Protokoll bei Streaming-Hardware mit begrenzten Ressourcen OpenVPN vorgezogen?

FALLSTUDIE 2: PROXYS FÜR TORRENT-NETZWERKE



Szenario: Ein P2P-Uploader möchte mit einer SOCKS5-Konfiguration seinen Standort verbergen, ohne den Aufwand einer vollständigen Datenverschlüsselung.

Diskussionsfrage: Vergleichen Sie die Abwägungen bei Sicherheit und Geschwindigkeit zwischen einem SOCKS5-Proxy und einem vollständigen IPVanish-VPN-Tunnel.

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

9	16	22	1	14	9	19	8		19	5	20	26	20		19	20	18	9	11	20
					1	21	6		14	15		12	15	7	19					

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: Welches Protokoll ist bei IPVanish voreingestellt?

Standardmäßig leitet es den Verkehr über das schnelle WireGuard.

Q2: Besitzt IPVanish seine Server-Hardware selbst?

Ja, es besitzt und verwaltet einen großen Teil seines physischen Servernetzwerks.

Q3: Wo hat IPVanish seinen Sitz?

Es hat seinen Sitz in den Vereinigten Staaten und unterliegt US-Recht.

Q4: Wie viele Geräte können sich gleichzeitig verbinden?

IPVanish bietet pro Konto unbegrenzt viele gleichzeitige Geräteverbindungen.

Q5: Werden Verbindungsprotokolle gespeichert?

Nein, es setzt eine strikte No-Logs-Richtlinie durch, die durch unabhängige Audits bestätigt wurde. [6]

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: Bietet IPVanish einen Proxy-Dienst an?

Ja, es stellt einen kostenlosen SOCKS5-Proxy für Torrenting bereit.

Q7: Ist ein Kill Switch enthalten?

Ja, ein Kill Switch ist unter Windows, macOS, Android und iOS verfügbar.

Q8: Kann ich mit IPVanish Geoblocking umgehen?

Ja, das weltweite Servernetzwerk ermöglicht den Zugriff auf eingeschränkte Mediatheken.

Q9: Unterstützt es Split-Tunneling?

Ja, Split Tunneling ist verfügbar, unter anderem unter Windows und Android.

Q10: Welche Verschlüsselungschiffren werden verwendet?

Es sichert Verbindungen mit AES-256- und ChaCha20-Verschlüsselung.

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 wird der SOCKS5-Proxy konfiguriert?

Er wird in Torrent-Clients eingerichtet, um die IP des Nutzers ohne den Overhead einer Verschlüsselung zu verbergen.

Q2: Wie verbessert eigene Server-Hardware die Sicherheit?

Es verringert die Risiken angemieteter Server von Dritten und gibt dem Anbieter direkte Kontrolle über die Serverkonfigurationen.

Q3: Welche Folgen hat die US-Rechtsordnung für den Datenschutz?

US-Gesetze schreiben zwar keine Vorratsdatenspeicherung vor, erlauben aber National Security Letters und Durchsuchungsbeschlüsse.

Q4: Wie verhindert der Kill Switch IP-Lecks?

Er blockiert alle Internetadapter, wenn die VPN-Verbindung unerwartet abbricht.

Q5: Welche Verschlüsselung wird mit WireGuard verwendet?

WireGuard nutzt symmetrische ChaCha20-Verschlüsselung und Poly1305-Authentifizierung. [7]

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: Wie wird die Zero-Logs-Richtlinie überprüft?

Die Leviathan Security Group hat es 2022 geprüft und Schellman 2025; keine der beiden fand Nutzerprotokolle. [3]

Q7: Wie geht es mit IPv6-DNS-Anfragen um?

Es leitet alle DNS- und IPv6-Anfragen automatisch über seine privaten Nameserver.

Q8: Bietet IPVanish Verschleierungsfunktionen?

Ja, die Scramble-Funktion verschleiert OpenVPN-Verkehr, um Firewalls zu umgehen.

Q9: Wie funktioniert Split-Tunneling auf Mobilgeräten?

Es ermöglicht ausgewählten Apps, den VPN-Tunnel zu umgehen und sich direkt zu verbinden.

Q10: Unterstützt es Router-Konfigurationen?

Ja, OpenVPN- und WireGuard-Konfigurationen können manuell auf DD-WRT-Router geladen werden. [1]

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

IPVanish besitzt den Großteil seiner Serverinfrastruktur, statt sie von Dritten zu mieten. [3]

2. VPN-EINBLICK

IPVanish ist seit 2012 tätig und gehört Ziff Davis, früher bekannt als J2 Global. [2]

3. VPN-EINBLICK

Der SOCKS5-Proxy verbirgt die öffentliche IP-Adresse des Clients, verschlüsselt die Datenpakete aber nicht.

4. VPN-EINBLICK

WireGuard ist das Standardprotokoll; OpenVPN und IKEv2/IPSec sind in den Apps ebenfalls verfügbar. [2]

5. VPN-EINBLICK

Das standardmäßige OpenVPN Scramble fügt den Paket-Headern eine XOR-Verschleierungsebene hinzu, um Firewalls zu umgehen.

6. VPN-EINBLICK

Dank der Richtlinie unbegrenzter gleichzeitiger Verbindungen können Nutzer alle Geräte ihres Haushalts gleichzeitig schützen. [2]

7. VPN-EINBLICK

Audits durch die Leviathan Security Group (2022) und Schellman (2025) bestätigten die No-Logs-Angaben. [3]

8. VPN-EINBLICK

Die Android-App unterstützt Einstellungen für ein dauerhaft aktives VPN (Always-on), die den Internetzugang verhindern, wenn der Tunnel getrennt ist.

9. VPN-EINBLICK

OpenVPN-Verbindungen können entweder UDP für Geschwindigkeit oder TCP für ein stabiles Routing durch Firewalls nutzen.

10. VPN-EINBLICK

Es bietet rund um die Uhr (24/7) Live-Chat-Support sowie telefonischen Support zu festen Geschäftszeiten an Werktagen. [5]

Technische Referenzen und Quellen

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

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] VPN.com. (2026). IPVanish Review.
https://www.vpn.com/vpn/ipvanish/

[2] Security.org. (2026). IPVanish VPN Review 2026.
https://www.security.org/vpn/ipvanish/review/

[3] All Things VPN. (2026). IPVanish Review 2026: Speeds, Streaming, & Privacy Tested.
https://allthingsvpn.com/ipvanish-review/

[4] Cloudwards. (2026). IPVanish Review 2026 [VPN Features, Pricing & Speed].
https://www.cloudwards.net/ipvanish-review/

[5] Top10VPN. (2026). IPVanish Review: Surprising Results from a Dark Horse.
https://www.top10vpn.com/reviews/ipvanish/

[6] IPVanish, Inc. (n.d.). IPVanish VPN: Fast & Secure [App Store listing].
https://apps.apple.com/us/app/ipvanish-vpn-fast-secure/id763638165

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

[8] Leech, M., et al. (1996). RFC 1928: SOCKS Protocol Version 5. IETF.
https://www.rfc-editor.org/rfc/rfc1928

[9] Nir, Y., & Langley, A. (2018). RFC 8439: ChaCha20 and Poly1305 for IETF Protocols. IETF.
https://www.rfc-editor.org/rfc/rfc8439

[10] Android Developers. (n.d.). VPN.
https://developer.android.com/develop/connectivity/vpn

Lösungsschlüssel: Kontrollpunkt 1 – Auswahlaufgaben

1 **WireGuard als Standard** WIREGUARD — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

WireGuard ist standardmäßig für optimierte Routing-Geschwindigkeiten eingestellt. Quelle: IPVanish Features.

2 **SOCKS5-Proxy** SOCKS5-PROXY — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

SOCKS5-Proxys verbergen den Standort der Clients ohne Mehraufwand durch Verschlüsselung. Quelle: IPVanish Support.

3 **Frage 3** — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

Die Leviathan Security Group führte 2022 das erste No-Logs-Audit von IPVanish durch; Schellman folgte 2025.

4 **US-Gerichtsbarkeit** VEREINIGTE STAATEN — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

IPVanish hat seinen Sitz in den Vereinigten Staaten und unterliegt den Regeln der Five-Eyes-Allianz. Quelle: IPVanish Review.

5 **Unbegrenzte Geräte** UNBEGRENZT — Richtige Antwort: A

HINWEIS FÜR LEHRKRÄFTE

IPVanish erlaubt unbegrenzt viele gleichzeitige Geräteverbindungen. Quelle: IPVanish Support.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 **Server-Hardware** EIGENES NETZWERK — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

IPVanish besitzt und verwaltet einen großen Teil seines physischen Servernetzes. Quelle: IPVanish Support.

7 **Frage 7** — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Falsch: Ein SOCKS5-Proxy verbirgt Ihre IP-Adresse, verschlüsselt die Daten aber nicht.

8 **Frage 8** — **Richtige Antwort: Falsch**

HINWEIS FÜR LEHRKRÄFTE

Falsch: IPVanish bietet in seinen Desktop- und Mobil-Apps einen Kill Switch.

9 **US-Gerichtsbarkeit** FIVE EYES USA — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

IPVanish hat seinen Sitz in den USA und unterliegt den Überwachungsregeln der Five Eyes. Quelle: IPVanish Review.

10 **Split Tunnel** GETEILTE ROUTE — **Richtige Antwort: Richtig**

HINWEIS FÜR LEHRKRÄFTE

Split Tunneling leitet den Verkehr bestimmter Apps außerhalb des sicheren Tunnels. Quelle: IPVanish Support.

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

B 1. WireGuard	H 2. SOCKS5-Proxy	D 3. Servergeschwindigkeit	A 4. Kill Switch
G 5. Geprüfte Protokolle	C 6. Gerätelimit	E 7. IP-Adresse	F 8. Sicherheit

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 WIREGUARD	2 SOCKS5-PROXY	3 SERVERLEISTUNG	4 KILL SWITCH
5 NO-LOGS-AUDIT	6 GERÄTELIMIT		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 B – SOCKSPROXY	2 H – SICHERHEIT	3 F – GERAETELIMIT	4 C – SERVERLEISTUNG
5 A – WIREGUARD	6 G – IPADRESSE	7 D – KILLSWITCH	8 E – NOLOGSAUDIT

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden WireGuard, SOCKS5-Proxy und Servergeschwindigkeit 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.

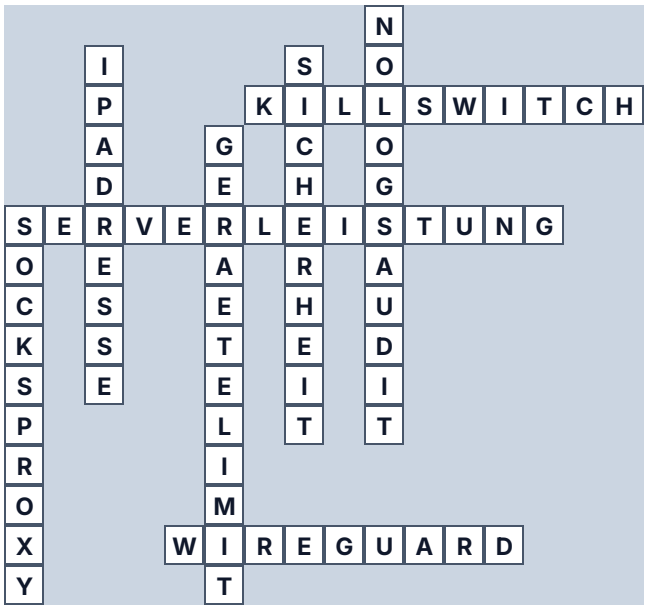
Quellenbewertung:
Lassen Sie die Lernenden mindestens eine Aussage anhand der Quellen des Arbeitsblatts prüfen und besprechen Sie, warum sich Zahlen, Preise und Regeln mit der Zeit ändern können.

Rätsellösungen und Hinweise für Lehrkräfte

LÖSUNG DES SUCHSELS

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

KREUZWORTRÄTSEL-LÖSUNG



LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

4 waagerecht: KILLSWITCH Ausfallsicherung, die den Internetverkehr blockiert, wenn das VPN ausfällt (10 Buchstaben)

6 waagerecht: SERVERLEISTUNG Durchsatzkapazität eines Serverknotens unter aktiver Last (14 Buchstaben)

7 waagerecht: WIREGUARD Open-Source-Protokoll, bekannt für Geschwindigkeit und moderne Kryptografie (9 Buchstaben)

SENKRECHT

1 senkrecht: NOLOGSAUDIT Geprüfte Nachweise, die bestätigen, dass keinerlei Nutzeraktivität erfasst wird (11 Buchstaben)

2 senkrecht: IPADRESSE Eindeutige Netzwerkkennung, die Geräten im Internet zugewiesen wird (9 Buchstaben)

3 senkrecht: SICHERHEIT Gesamtes Schutzniveau des verschlüsselten Tunnelsystems (10 Buchstaben)

5 senkrecht: GERAETELIMIT Beschränkung der Anzahl aktiver Gerätesitzungen (12 Buchstaben)

6 senkrecht: SOCKSPROXY Unverschlüsseltes Proxy-System (SOCKS5), mit dem die Standorte von P2P-Clients verschleiert werden (10 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. UGEIWARDR — **WIREGUARD**
2. EERRLNSUEGSTIV — **SERVERLEISTUNG**
3. NASULOITGDO — **NOLOGSAUDIT**
4. RESDSEIPA — **IPADRESSE**
5. OPYOKRSSXC — **SOCKSPROXY**
6. CSLITKIWHL — **KILLSWITCH**
7. LIEGEETMIRTA — **GERAETELIMIT**
8. IHRTSEIHEC — **SICHERHEIT**

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"IPVANISH SETZT STRIKT AUF NO LOGS"

Lösungsschlüssel zu den Fallstudien

A FALLSTUDIE 1: KONFIGURATION EINES MEDIACENTERS

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein Kunde möchte seinen Android-basierten Fire-TV-Mediaplayer mit IPVanish absichern, um sicher zu streamen und dabei einen hohen Durchsatz beizubehalten.
- Empfohlene Strategie und Lösung: Bewertungshinweise: Es sollte erklärt werden, dass WireGuard eine kleinere Codebasis hat, im Kernel-Space arbeitet und weniger CPU-Zyklen benötigt, was die Geschwindigkeit auf leistungsschwacher Hardware maximiert.

B FALLSTUDIE 2: PROXYS FÜR TORRENT-NETZWERKE

Lösung für Lehrkräfte

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Szenarioanalyse: Ein P2P-Uploader möchte mit einer SOCKS5-Konfiguration seinen Standort verbergen, ohne den Mehraufwand einer vollständigen Datenverschlüsselung.
- Empfohlene Strategie und Lösung: Bewertungshinweise: Es sollte festgehalten werden, dass SOCKS5 die IP-Adresse verbirgt, ohne den Datenverkehr zu verschlüsseln, was höhere Geschwindigkeiten, aber keinerlei Schutz der Privatsphäre gegenüber der Paketinspektion durch den ISP bietet.