Name: _____ Datum: _____ Punkte: _____

Proxy oder VPN Arbeitsblatt

Vergleich von Proxyservern und virtuellen privaten Netzwerken, Unterschieden bei der Verschlüsselung sowie Routing auf Anwendungs-vs. Systemebene

VPN-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 Grundprinzipien virtueller privater Netzwerke (VPNs). Sie erfahren, wie verschlüsselte Tunnel Ihre Daten schützen, wie Netzwerkprotokolle funktionieren und wie man Datenlecks bei der Privatsphäre erkennt und eindämmt.

KONTROLLPUNKTE DES ARBEITSBLATTS

- [ ] **Teil 1-4: VPN-Konzepte und -Protokolle 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.**

VPN-Leitfaden von VPN.com öffnen

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

Ihr Lernfahrplan: VPN

- Stellen Sie Anwendungs-Proxys der systemweiten VPN-Verschlüsselung gegenüber.
- Die Fähigkeiten von SOCKS5 im Vergleich zu einfachen HTTP-Proxys bestimmen.
- Analysieren Sie, wie browserbasierte Proxys Hintergrund-Apps ungeschützt lassen.
- Verstehen, wie ISPs unverschlüsselten Datenverkehr in Proxy-Tunneln protokollieren.
- Wählen Sie das passende Routing-Werkzeug entsprechend den Anforderungen an Geschwindigkeit und Sicherheit.

ANLEITUNG ZUM ARBEITSBLATT PROXY-VERGLEICH

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: Vergleich von Proxys und VPNs. Zum Schluss folgt die Bonusaufgabe Schnell denken.

PROXY ODER VPN (EINFÜHRUNG)

Proxys und VPNs erfüllen unterschiedliche Aufgaben für die digitale Privatsphäre. Ein Proxyserver ist eine Umleitung auf Anwendungsebene, die Ihre IP-Adresse für bestimmte Programme verbirgt, ohne die Daten zu verschlüsseln. Ein VPN arbeitet auf Netzwerkebene und sichert den gesamten Systemverkehr durch Verschlüsselung. Welches Werkzeug das richtige ist, hängt von Ihren Sicherheitsanforderungen ab.

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

Kontrollpunkt 1: Auswahlaufgaben

1. Auf welcher Schicht des OSI-Modells arbeitet ein Standard-HTTP-Proxy?

- A. Physische Schicht
- B. Netzwerkschicht
- C. Anwendungsschicht
- D. Sicherungsschicht (Data Link Layer)

2. Was ist ein wesentlicher Protokollvorteil von SOCKS5 gegenüber normalen HTTP-Proxys?

- A. Es erzwingt die vollständige Verschlüsselung der Nutzdaten
- B. Es unterstützt das Routing beliebigen TCP/UDP-Verkehrs
- C. Es ist immun gegen DNS-Leaks
- D. Es arbeitet direkt im Kernel-Space

3. Warum ist ein VPN in der Regel sicherer als ein Proxyserver?

- A. Es läuft auf schnellerer entfernter Hardware
- B. Es verschlüsselt den gesamten Netzwerkverkehr systemweit
- C. Es benötigt keine lokalen Routingtabellen
- D. Es beseitigt die Netzwerklatenz vollständig

4. Welcher Proxy-Typ leitet den Datenverkehr standardmäßig ganz ohne Verschlüsselung um?

- A. Ein einfacher HTTP-Proxy
- B. Ein verschlüsselter HTTPS-Proxy
- C. Ein sicherer WireGuard-Client
- D. Ein verschleierter VPN-Server

5. Was passiert mit dem Datenverkehr von Hintergrundanwendungen, wenn ein Browser-Proxy verwendet wird?

- A. Es wird automatisch verschlüsselt
- B. Es wird vom Proxyserver blockiert
- C. Es wird durch den Proxy-Tunnel geleitet
- D. Es umgeht den Proxy und legt Ihre IP offen

Kontrollpunkt 2: Richtig oder falsch

6 Frage 6

6. Ein SOCKS5-Proxy verschlüsselt alle Paketnutzdaten, die über den Server laufen.

Richtig Falsch

7 Frage 7

7. Ein VPN arbeitet auf der Netzwerkebene und sichert den gesamten Systemverkehr.

Richtig Falsch

8 Frage 8

8. Proxys sind im Allgemeinen schneller als VPNs, weil sie eine tiefe Paketverschlüsselung durchführen.

Richtig Falsch

9 Frage 9

9. Für die Konfiguration eines Proxys müssen Umleitungen des Datenverkehrs innerhalb bestimmter Apps eingerichtet werden.

Richtig Falsch

10 Frage 10

10. Ein Proxy schützt Ihren Datenverkehr nicht vor Tracking durch den lokalen ISP.

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. Ein _____ auf Anwendungsebene leitet bestimmten Browser-Datenverkehr um, ohne andere Apps abzusichern.

2. Ein robuster _____ kapselt und verschlüsselt alle Datenpakete des Geräts.

3. Das Protokoll _____ liegt zwischen Anwendungs- und Transportschicht.

4. HTTP-Proxys arbeiten im OSI-Modell auf _____ .

5. Gewöhnlichen Proxyservern fehlt die _____ der Nutzdaten, sodass die Daten angreifbar bleiben.

6. Der Schutz eines VPN wirkt _____ für alle Netzwerkadapter.

WORTSCHATZ-WORTBANK

HTTP-PROXY SCHICHT SIEBEN SICHTBARKEIT SOCKS5 SYSTEMWEIT
UDP-SUPPORT VERSCHLÜSSELUNG VPN-TUNNEL

Schreiben Sie Ihre Antworten hier:

1. **2.**

3. **4.**

5. **6.**

Kontrollpunkt 4: Zuordnung von Netzwerk-Begriffen

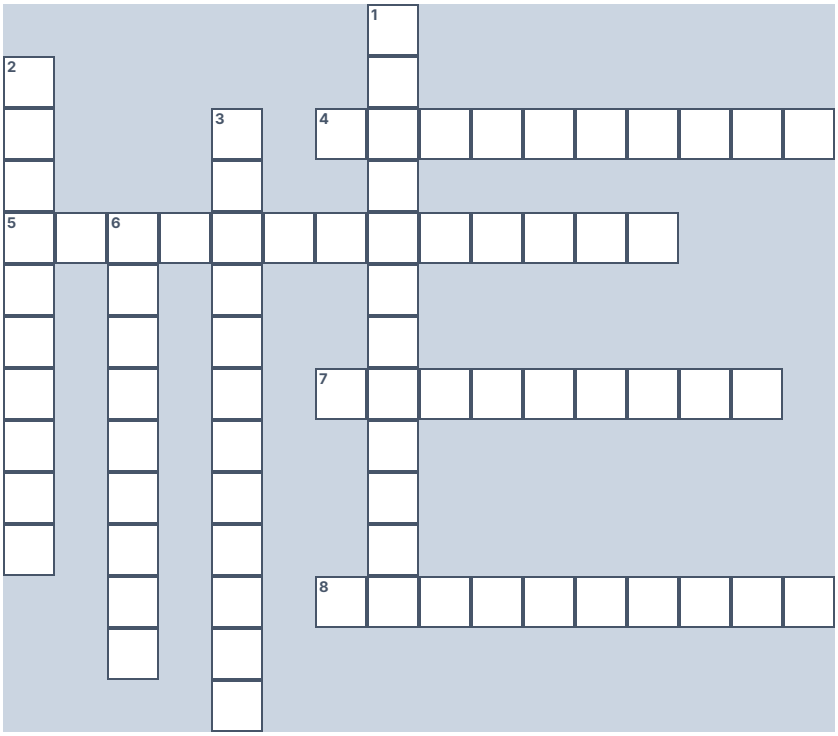
DEFINITIONEN ZUORDNEN

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

☐	1. HTTP-Proxy	A	Routing auf Betriebssystemebene, das den Datenverkehr aller Anwendungen verschlüsselt.
☐	2. SOCKS5-Proxy	B	Die Anwendungsschicht, auf der Standard-Webproxy-Protokolle arbeiten.
☐	3. VPN-Tunnel	C	Die Fähigkeit von SOCKS5, neben TCP auch UDP weiterzuleiten, anders als einfache HTTP-Proxys.
☐	4. Systemweit	D	Client-Erweiterung, die nur den Datenverkehr innerhalb der Browser-Sandbox verbirgt.
☐	5. OSI-Schicht 7	E	Verschlüsselung und Kapselung des gesamten Hintergrundverkehrs des Geräts.
☐	6. UDP-Unterstützung	F	Zustand des Datenverkehrs, in dem unverschlüsselte Proxy-Daten für ISPs sichtbar bleiben.
☐	7. Browser-Proxy	G	Proxy auf Anwendungsebene, der den Datenverkehr bestimmter Webbrowser umleitet.
☐	8. Sichtbarkeit für den ISP	H	Proxy-Protokoll zwischen Anwendungs- und Transportschicht, ohne Verschlüsselung.

Kontrollpunkt 5: Kreuzworträtsel

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



WAAGERECHT

4. Proxy-Protokoll zwischen Anwendungs- und Transportschicht, ohne Verschlüsselung (10)

5. Die Anwendungsschicht, auf der Standard-Webproxy-Protokolle arbeiten (13)

7. Verschlüsselung und Kapselung, die den gesamten Hintergrundverkehr eines Geräts umschließt (9)

8. Routing auf Betriebssystemebene, das den Datenverkehr aller Anwendungen verschlüsselt (10)

SENKRECHT

1. Client-Erweiterung, die nur den Datenverkehr innerhalb der Browser-Sandbox verbirgt (12)

2. Fähigkeit von SOCKS5, anders als einfache HTTP-Proxys neben TCP auch UDP weiterzuleiten (10)

3. Zustand, in dem unverschlüsselte Proxy-Daten für Internetanbieter einsehbar bleiben (12)

6. Proxy auf Anwendungsebene, der den Datenverkehr bestimmter Webbrowser umleitet (9)

Kontrollpunkt 5, Alternative: Barrierefreie Kreuzworträtsel-Hinweise

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

WAAGERECHT

4 waagerecht: Proxy-Protokoll zwischen Anwendungs- und Transportschicht, ohne Verschlüsselung (10 Buchstaben):

5 waagerecht: Die Anwendungsschicht, auf der Standard-Webproxy-Protokolle arbeiten (13 Buchstaben):

7 waagerecht: Verschlüsselung und Kapselung, die den gesamten Hintergrundverkehr eines Geräts umschließt (9 Buchstaben):

8 waagerecht: Routing auf Betriebssystemebene, das den Datenverkehr aller Anwendungen verschlüsselt (10 Buchstaben):

SENKRECHT

1 senkrecht: Client-Erweiterung, die nur den Datenverkehr innerhalb der Browser-Sandbox verbirgt (12 Buchstaben):

2 senkrecht: Fähigkeit von SOCKS5, anders als einfache HTTP-Proxys neben TCP auch UDP weiterzuleiten (10 Buchstaben):

3 senkrecht: Zustand, in dem unverschlüsselte Proxy-Daten für Internetanbieter einsehbar bleiben (12 Buchstaben):

6 senkrecht: Proxy auf Anwendungsebene, der den Datenverkehr bestimmter Webbrowser umleitet (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.

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

WORTSCHATZ-WORTLISTE

HTTPPROXY SOCKSPROXY VPNTUNNEL SYSTEMWEIT SCHICHTSIEBEN
UDPSUPPORT BROWSERPROXY SICHTBARKEIT

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. HTTPPROXY**
- **B. SOCKSPROXY**
- **C. VPNTUNNEL**
- **D. SYSTEMWEIT**
- **E. SCHICHTSIEBEN**
- **F. UDPSUPPORT**
- **G. BROWSERPROXY**
- **H. SICHTBARKEIT**

DEFINITIONEN UND ZUORDNUNGSFELDER

_____ 1. Die Anwendungsschicht, auf der Standard-Webproxy-Protokolle arbeiten.

_____ 2. Fähigkeit von SOCKS5, anders als einfache HTTP-Proxys neben TCP auch UDP weiterzuleiten.

_____ 3. Proxy auf Anwendungsebene, der den Datenverkehr bestimmter Webbrowser umleitet.

_____ 4. Client-Erweiterung, die nur den Datenverkehr innerhalb der Browser-Sandbox verbirgt.

_____ 5. Verschlüsselung und Kapselung, die den gesamten Hintergrundverkehr eines Geräts umschließt.

_____ 6. Routing auf Betriebssystemebene, das den Datenverkehr aller Anwendungen verschlüsselt.

_____ 7. Zustand, in dem unverschlüsselte Proxy-Daten für Internetanbieter einsehbar bleiben.

_____ 8. Proxy-Protokoll zwischen Anwendungs- und Transportschicht, ohne Verschlüsselung.

Kontrollpunkt 7: Buchstabensalat

Bringen Sie die Buchstaben unten in die richtige Reihenfolge, um zentrale VPN-Begriffe aufzudecken. Schreiben Sie Ihre Antworten in die ausfüllbaren Eingabefelder.

1. RPPTHOXYT
2. LVETPNNUN
3. CSSEIENHTC HBI
4. XPSORYEORB RW
5. OPYOKRSSXC
6. IETWESYMTS
7. DSUPPORTUP
8. RCTEATSBIIK H

Bonusaufgabe: Schnell denken

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

1	Unterschiede zwischen einem Proxy und einem VPN			
2	Dinge, die ohne VPN unverschlüsselt bleiben			
3	Möglichkeiten, ein gefälschtes WLAN zu erkennen			
4	Dinge, die ein Vermittler im Alltag erledigt			
5	Situationen, in denen ein Proxy ausreicht			
6	Geräte, die ein VPN nutzen können			
7	Proxy-Arten, die Sie kennen			
8	Dinge, die ein VPN verbergen kann			
9	Mythen über VPNs			
10	Versprechen, die ein guter VPN-Anbieter gibt			
11	Dinge, vor denen ein VPN Sie nicht schützen kann			
12	Wörter aus diesem Arbeitsblatt, die Sie sich merken möchten			
13	Gründe, auf Reisen ein VPN zu nutzen			
14	Situationen, in denen Sie ein VPN möchten			
15	Orte, an denen Sie ein VPN nutzen würden			

Kontrollpunkt 8: Fallstudien zu VPNs

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

SARAH (STUDENTIN IM CAFÉ)

👩‍💻 „Hallo! Ich bin bei Coffee & Bytes in einem offenen Netzwerk namens 'Free_Wi-Fi_No_Password'. Ich muss mich in meinem Schul-E-Mail-Konto anmelden, und eine Freundin sagt, ein kostenloser Browser-Proxy reiche aus, um sicher zu bleiben. Würde ein Proxy meine Anmeldung und meine Dateien schützen, oder brauche ich ein VPN?“

ALEX (REISENDER STUDENT)

👩‍💻 „Ich bin im Ausland, und bei einer Biologie-Dokumentation, die in meinem Heimatland gehostet wird, steht 'Dieses Video ist an Ihrem aktuellen Standort nicht verfügbar.' Ein Mitschüler nutzt einen Proxy, und ich habe ein VPN. Warum werde ich blockiert, und welches Werkzeug würde besser funktionieren?“

Kontrollpunkt 9: Entschlüsselung der Chiffre

Um Ihr Training zum Proxy-Vergleich abzuschließen, entschlüsseln Sie diese geheime Nachricht über sicheres Tunneling.

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

12 5 9 20 5 14 19 9 5 9 8 18 5 14

4 1 20 5 14 22 5 18 11 5 8 18 21 5 2 5 18

5 9 14 5 14 16 18 15 24 25

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 an, die Interessenten zur Nutzung virtueller privater Netzwerke haben.

Q1: Was ist ein VPN und wie funktioniert es?

Ein Virtual Private Network (VPN) verschlüsselt Ihre Internetverbindung und leitet Ihren Datenverkehr über einen sicheren entfernten Server. Dadurch wird Ihre öffentliche IP-Adresse verschleiert, und es wird eingeschränkt, was Beobachter im lokalen Netzwerk und Ihr ISP über den durch den VPN-Tunnel geleiteten Datenverkehr sehen können.

Q2: Was ist ein Proxyserver?

Ein Proxyserver ist ein Vermittler, der Anfragen zwischen Ihrer Anwendung und dem Zielserver weiterleitet. Die Website sieht die IP-Adresse des Proxys statt Ihrer eigenen, aber umgeleitet wird nur der Datenverkehr von Apps, die für den Proxy konfiguriert sind, und ein einfacher Proxy verschlüsselt diesen Datenverkehr nicht.

Q3: Macht mich ein VPN online vollständig anonym?

Nein. Ein VPN verbirgt zwar Ihre IP-Adresse und verschlüsselt den Datenverkehr, Sie können aber weiterhin über Browser-Cookies, angemeldete Konten (wie Google oder Facebook) und Browser-Fingerprinting verfolgt werden oder wenn Ihr VPN-Anbieter Ihre Daten protokolliert.

Q4: Verlangsamt ein VPN meine Internetgeschwindigkeit?

Ja, leicht. Der Verschlüsselungsvorgang und die räumliche Entfernung zum VPN-Server erhöhen Latenz und Overhead. Die Auswirkung hängt von Anbieter, Protokoll, Serverentfernung, Gerät und Netzwerkbedingungen ab.

Q5: Ist ein Proxy ein VPN?

Nein. Ein Proxy leitet den Datenverkehr bestimmter Apps weiter, meist ohne Verschlüsselung. Ein VPN baut auf der Netzwerkschicht einen verschlüsselten Tunnel auf, der den gesamten Datenverkehr des Geräts transportiert, auch den von Hintergrund-Apps.

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

Sehen Sie sich die häufigsten Fragen und Antworten an, die Interessenten zur Nutzung virtueller privater Netzwerke haben.

Q6: Kann ich einen kostenlosen Proxy verwenden?

Das ist möglich, aber kostenlose Proxys werden oft von unbekannten Betreibern geführt. Da ein einfacher Proxy den Datenverkehr nicht verschlüsselt, kann sein Betreiber unverschlüsselte Seiten einsehen und sogar verändern. Prüfen Sie vor der Nutzung, wer den Dienst betreibt.

Q7: Speichert ein Proxy Protokolle?

Das ist möglich. Ein Proxy verarbeitet jede Anfrage, die er weiterleitet, daher kann sein Betreiber Ihre IP-Adresse, die besuchten Websites und den Zeitpunkt aufzeichnen. Prüfen Sie, wer ihn betreibt und was seine Datenschutzrichtlinie besagt.

Q8: Wann reicht ein Proxy aus?

Für Aufgaben mit geringem Risiko, etwa um den scheinbaren Standort eines Browsers zu ändern, kann ein Proxy ausreichen. Für Online-Banking, öffentliches WLAN oder den Schutz aller Apps auf einem Gerät ist ein VPN die sicherere Wahl, weil es den gesamten Datenverkehr verschlüsselt.

Q9: Kann ein Proxy alle Apps auf meinem Smartphone schützen?

Nein. Nur Apps, die die Proxy-Einstellung beachten, nutzen ihn; alle anderen verbinden sich direkt. Eine VPN-App leitet dagegen alle Apps des Telefons durch ihren verschlüsselten Tunnel.

Q10: Was ist ein SOCKS5-Proxy?

SOCKS5, definiert in RFC 1928, ist ein Proxyprotokoll, das zwischen der Anwendungs- und der Transportschicht angesiedelt ist. Es kann TCP-Verbindungen und UDP-Datagramme weiterleiten und unterstützt Authentifizierung, besitzt aber keine integrierte Verschlüsselung. [1]

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

Erkunden Sie technische und strukturelle Aspekte virtueller privater Netzwerke und sicherer Tunnelprotokolle.

Q1: Auf welchen Netzwerkschichten arbeiten Proxys und VPNs?

Ein HTTP-Proxy arbeitet auf der Anwendungsschicht (Schicht 7) und versteht Webanfragen. SOCKS5 liegt zwischen Anwendungs- und Transportschicht. VPN-Protokolle wie IPsec oder WireGuard arbeiten auf der Netzwerkschicht und können daher den gesamten IP-Verkehr des Geräts transportieren.

Q2: Bleibt eine HTTPS-Seite über einen Proxy verschlüsselt?

Ja. Wenn Sie eine HTTPS-Website über einen Proxy aufrufen, läuft die TLS-Verschlüsselung Ende-zu-Ende zwischen Ihrem Browser und der Website, sodass der Proxy zwar die Domain, aber nicht den Seiteninhalt sieht. Einfache HTTP-Seiten bleiben lesbar.

Q3: Was sind WebRTC-Lecks und wie verhindert ein VPN sie?

WebRTC ist ein Browserprotokoll, das Ihre echte lokale und öffentliche IP-Adresse preisgeben kann, selbst wenn ein VPN aktiv ist. Premium-VPNs blockieren oder fälschen WebRTC-Anfragen in ihren Desktop- und Mobil-Apps sowie Browsererweiterungen.

Q4: Was ist ein transparenter Proxy und wer verwendet ihn?

Ein transparenter Proxy fängt Datenverkehr ab, ohne dass auf dem Gerät des Nutzers etwas eingerichtet wird. Schulen, Unternehmen und ISPs setzen solche Proxys zum Zwischenspeichern oder Filtern von Inhalten ein. Nutzer wissen oft nicht, dass einer aktiv ist, und er bietet ihnen keine Privatsphäre.

Q5: Wie umgeht Verschleierung (Obfuscation) VPN-Sperren?

Verschleierung (oder „Stealth VPN“) tarnt VPN-Verkehr so, dass er wie gewöhnlicher HTTPS-Verkehr (Port 443) aussieht. Das kann helfen, die Deep Packet Inspection (DPI) zu umgehen, mit der Regierungen oder Schul- und Firmennetzwerke VPNs blockieren.

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

Erkunden Sie technische und strukturelle Aspekte virtueller privater Netzwerke und sicherer Tunnelprotokolle.

Q6: Was ist Split-Tunneling und wann sollte ich es verwenden?

Mit Split Tunneling legen Sie fest, welche Apps durch den verschlüsselten VPN-Tunnel geleitet werden und welche sich direkt mit dem Internet verbinden. Nutzen Sie es, um sensible Banking-Apps durch das VPN zu leiten, während lokale Spiele sich direkt verbinden und so die zusätzliche Latenz durch das VPN vermeiden.

Q7: Warum kann sich ein Proxy schneller anfühlen als eine VPN-Verbindung?

Ein einfacher Proxy verzichtet auf Verschlüsselung und verarbeitet nur den Datenverkehr einer App, daher fällt weniger Rechenaufwand an. Ein VPN verschlüsselt jedes Paket des Geräts. Mit modernen Protokollen ist der Unterschied oft gering, und der Proxy bietet weit weniger Schutz.

Q8: Können Websites erkennen, dass ich einen Proxy oder ein VPN verwende?

Oft ja. Viele Websites gleichen IP-Adressen mit Listen bekannter Proxy- und VPN-Server ab, und HTTP-Proxys können Header wie Via oder X-Forwarded-For hinzufügen. Streamingdienste blockieren häufig beides.

Q9: Was ist der Schutz vor DNS-Lecks?

Der DNS-Leak-Schutz sorgt dafür, dass Ihr Gerät Suchanfragen nach Websites (DNS-Anfragen) über die privaten, verschlüsselten DNS-Server des VPN statt über die Server Ihres Internetanbieters sendet. So wird verhindert, dass Ihr Internetanbieter nachverfolgt, welche Websites Sie besuchen.

Q10: Kann ein Proxy die Drosselung durch den Internetanbieter verhindern?

Selten. Ein einfacher Proxy verschlüsselt den Traffic nicht, daher kann der Internetanbieter weiterhin erkennen, um welche Art von Aktivität es sich handelt. Ein VPN verbirgt die Art des Traffics, aber keines der beiden Tools behebt Überlastungen oder Datenvolumenbegrenzungen.

Teil 11: 10 interessante VPN-Fakten und Einblicke aus der Praxis

Lernen Sie diese besonders wertvollen, realen Fakten und Erkenntnisse zur Geschichte, zum Markt und zur Technologie von VPNs kennen.

1. SOCKS-STANDARD

Das SOCKS-Protokoll Version 5 wurde im März 1996 von der IETF als RFC 1928 veröffentlicht und ist bis heute die maßgebliche Spezifikation für SOCKS5-Proxys, die von Browsern und Apps genutzt werden. [1]

2. SHIM-SCHICHT

RFC 1928 beschreibt SOCKS als Zwischenschicht (Shim) zwischen Anwendungs- und Transportschicht; daher kann es keinen Traffic der Netzwerkschicht wie ICMP weiterleiten. [1]

3. UDP-RELAY

SOCKS5 führte den Befehl UDP ASSOCIATE ein, mit dem ein Proxy neben TCP-Verbindungen auch UDP-Datagramme weiterleiten kann, was einfache HTTP-Proxys nicht leisten. [1]

4. STANDARD-SOCKS-PORT

SOCKS5-Clients verbinden sich laut RFC 1928 standardmäßig über TCP-Port 1080 mit dem Proxyserver; bei vielen Proxydiensten können Nutzer andere Ports wählen. [1]

5. HTTP-VERMITTLER

Der HTTP-Standard (RFC 9110) definiert einen Proxy als vom Client gewählten Vermittler, der Nachrichten weiterleitet und Anfragen an den Ursprungsserver übermittelt.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) untersucht Paketinhalte und Verkehrsmuster; unverschlüsselter Proxy-Datenverkehr ist für sie vollständig sichtbar, während VPN-Datenverkehr weit weniger preisgibt.

7. VPNS AUF NETZWERKEBENE

IPsec, beschrieben in NIST SP 800-77, schützt den Datenverkehr auf der Netzwerkschicht, sodass die IP-Pakete jeder Anwendung ohne Einrichtung pro App gesichert werden können. [2]

8. NUR IM BROWSER WIRKSAM

Ein in einem Browser eingerichteter Proxy wirkt nur auf diesen Browser; E-Mail-Programme, Spiele und Systemupdates nutzen weiterhin die normale Verbindung des Geräts.

9. TOR VS. PROXYS

Tor leitet den Datenverkehr über drei von Freiwilligen betriebene Relays (Guard, Middle und Exit) und wird meist über einen lokalen SOCKS-Proxy angesprochen; so entstehen Schichten, die ein einzelner Proxy nicht bieten kann.

10. KOMPROMISS BEI DER GESCHWINDIGKEIT

Proxys können schneller wirken, weil sie auf Verschlüsselung verzichten, aber moderne VPN-Protokolle wie WireGuard verursachen wenig Overhead und schützen dabei den gesamten Geräteverkehr.

Technische Referenzen und Quellen

Zitierte Veröffentlichungen, kryptografische Spezifikationen und offizielle Dokumentstandards, die in diesem Arbeitsblatt verwendet werden.

WISSENSCHAFTLICHE UND FACHLICHE QUELLEN

[1] IETF. (1996). RFC 1928: SOCKS Protocol Version 5.
https://datatracker.ietf.org/doc/html/rfc1928

[2] NIST. (2020). SP 800-77 Rev. 1: Guide to IPsec VPNs.
https://csrc.nist.gov/pubs/sp/800/77/r1/final

[3] WireGuard. (n.d.). WireGuard: fast, modern, secure VPN tunnel.
https://www.wireguard.com/

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

[5] OpenVPN. (n.d.). OpenVPN 2.6 Manual.
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

Lösungsschlüssel: Vergleich von Proxyservern und virtuellen privaten Netzwerken, Unterschiede bei der Verschlüsselung und Routing pro Anwendung oder systemweit

1 **OSI-Schicht eines Proxys** PROTOKOLLE — **Richtige Antwort: C**

HINWEIS FÜR LEHRKRÄFTE

Herkömmliche HTTP/HTTPS-Proxys arbeiten auf der Anwendungsschicht (Layer 7) und leiten bestimmten Browserverkehr um. Ein systemweites Netzwerk-Routing bieten sie nicht. Quelle: Tor Project Foundation.

2 **Frage 2** — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

SOCKS5 leitet TCP- und UDP-Datenverkehr zwischen Anwendungs- und Transportschicht weiter, verschlüsselt aber standardmäßig nicht, während HTTP-Proxys Webanfragen verarbeiten.

3 **VPN-Systemverschlüsselung** WLAN-SICHERHEIT — **Richtige Antwort: B**

HINWEIS FÜR LEHRKRÄFTE

Ein VPN kapselt und verschlüsselt den gesamten Datenverkehr des Betriebssystems systemweit, während ein Proxy nur den Datenverkehr bestimmter konfigurierter Anwendungen umleitet. Quelle: Deloitte Advisory.

4 **Fehlende Proxy-Verschlüsselung** ROUTING-STEUERUNG — **Richtige Antwort: A**

HINWEIS FÜR LEHRKRÄFTE

HTTP-Proxys leiten Browserverkehr auf der Anwendungsschicht weiter, ohne die Paketnutzdaten zu verschlüsseln; Ihr Netzwerkbetreiber oder ISP kann Ihren Datenverkehr also weiterhin nachverfolgen. Quelle: IETF Proxy Vulnerabilities.

5 **Umgehungsschwachstelle** PRIVATSPHÄRE — **Richtige Antwort: D**

HINWEIS FÜR LEHRKRÄFTE

Browser-Proxys wenden Regeln nur auf den Webbrowser selbst an. Hintergrund-Apps, Betriebssystem-Updates und E-Mail-Clients umgehen den Proxy und legen Ihre eigentliche IP-Adresse offen. Quelle: W3C Consortium.

Lösungsschlüssel: Kontrollpunkt 2 – Richtig oder Falsch

6 Frage 6

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

SOCKS5 leitet Datenverkehr zwischen Anwendungs- und Transportschicht weiter, verschlüsselt aber standardmäßig nicht, sodass Paketinhalte während der Übertragung lesbar bleiben.

7 Tunnel auf der Netzwerkschicht GESCHWINDIGKEITEN

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Da ein VPN auf der Netzwerkschicht arbeitet, leitet und verschlüsselt es den ausgehenden Verkehr Ihres Geräts und hilft so, den Datenverkehr systemweit zu schützen. Quelle: Deloitte Advisory.

8 Verschlüsselungsgrenze von Proxys SNIFFING-RISIKO

Richtige Antwort: Falsch

HINWEIS FÜR LEHRKRÄFTE

Proxys können manchmal schneller sein, aber nur, weil sie KEINE Verschlüsselung durchführen. Durch die fehlende Verschlüsselung können Daten mitgelesen werden. Quelle: IETF Proxy Vulnerabilities.

9 Umleitung auf App-Ebene FIREWALLS

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Anders als systemweite VPNs müssen Proxyserver manuell in den Browsereinstellungen oder in anwendungsspezifischen Proxyfeldern eingerichtet werden. Quelle: W3C Consortium.

10 Risiko der Nachverfolgung durch den ISP NO-LOGS

Richtige Antwort: Richtig

HINWEIS FÜR LEHRKRÄFTE

Da Standard-HTTP-/SOCKS5-Proxys die Nutzdaten nicht verschlüsseln, behält Ihr lokaler Internetanbieter vollen Einblick in Ihre Online-Aktivitäten. Quelle: EDRi Retention Guidelines.

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. HTTP-Proxy	H 2. SOCKS5-Proxy	E 3. VPN-Tunnel	A 4. Systemweit
B 5. OSI-Schicht 7	C 6. UDP-Unterstützung	D 7. Browser-Proxy	F 8. Sichtbarkeit für den ISP

KONTROLLPUNKT 3: LÖSUNG SCHLÜSSELBEGRIFFE

1 HTTP-PROXY	2 VPN-TUNNEL	3 SOCKS5	4 SCHICHT SIEBEN
5 VERSCHLÜSSELUNG	6 SYSTEMWEIT		

KONTROLLPUNKT 6, ALTERNATIVE: LÖSUNG WORTZUORDNUNG

1 E – SCHICHTSIEBEN	2 F – UDPSUPPORT	3 A – HTTPPROXY	4 G – BROWSERPROXY
5 C – VPNTUNNEL	6 D – SYSTEMWEIT	7 H – SICHTBARKEIT	8 B – SOCKSPROXY

DISKUSSIONSHINWEISE FÜR LEHRKRÄFTE

Schlüsselbegriffe:
Prüfen Sie, ob die Lernenden HTTP-Proxy, SOCKS5-Proxy und VPN-Tunnel 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

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

KREUZWORTRÄTSEL-LÖSUNG

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

LEITFADEN FÜR LEHRKRÄFTE ZU DEN KREUZWORTRÄTSEL-LÖSUNGEN

WAAGERECHT

4 waagerecht: SOCKSPROXY Proxy-Protokoll zwischen Anwendungs- und Transportschicht, ohne Verschlüsselung (10 Buchstaben)

5 waagerecht: SCHICHTSIEBEN Die Anwendungsschicht, auf der Standard-Webproxy-Protokolle arbeiten (13 Buchstaben)

7 waagerecht: VPNTUNNEL Verschlüsselung und Kapselung, die den gesamten Hintergrundverkehr eines Geräts umschließt (9 Buchstaben)

8 waagerecht: SYSTEMWEIT Routing auf Betriebssystemebene, das den Datenverkehr aller Anwendungen verschlüsselt (10 Buchstaben)

SENKRECHT

1 senkrecht: BROWSERPROXY Client-Erweiterung, die nur den Datenverkehr innerhalb der Browser-Sandbox verbirgt (12 Buchstaben)

2 senkrecht: UDPSUPPORT Fähigkeit von SOCKS5, anders als einfache HTTP-Proxys neben TCP auch UDP weiterzuleiten (10 Buchstaben)

3 senkrecht: SICHTBARKEIT Zustand, in dem unverschlüsselte Proxy-Daten für Internetanbieter einsehbar bleiben (12 Buchstaben)

6 senkrecht: HTTPPROXY Proxy auf Anwendungsebene, der den Datenverkehr bestimmter Webbrowser umleitet (9 Buchstaben)

Lösungsschlüssel für Buchstabensalat und Chiffre

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

LÖSUNGSSCHLÜSSEL BUCHSTABENSALAT

1. RPPTHOXYT — HTTPPROXY
2. LVETPNNUN — VPNTUNNEL
3. CSSEIENHTCHBI — SCHICHTSIEBEN
4. XPSORYEORBRW — BROWSERPROXY
5. OPYOKRSSXC — SOCKSPROXY
6. IETWESYMTS — SYSTEMWEIT
7. DSUPPORTUP — UDPSUPPORT
8. RCTEATSBIIKH — SICHTBARKEIT

LÖSUNGSSCHLÜSSEL ZUR GEHEIMEN CHIFFRE-AUFGABE

"LEITEN SIE IHREN DATENVERKEHR UEBER EINEN PROXY"

Lösungsschlüssel zu den Fallstudien

A Szenario A: Sicherheit in öffentlichen Netzwerken

SNIFFING UND VERSCHLÜSSELUNG

Sarahs Dilemma

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Risiken: Packet Sniffing, Abfangen von Daten und Man-in-the-Middle-Angriffe. Jemand im selben Café-Netzwerk könnte ihre Anmeldedaten oder ihre Hausaufgabendatei abfangen.
- Proxy oder VPN: Ein einfacher Browser-Proxy verschlüsselt ihren Datenverkehr nicht. Ein VPN verschlüsselt alles auf dem Gerät, sodass abgefangene Pakete für Schnüffler vor Ort unlesbar sind.

B Szenario B: Zugriff auf gesperrte Ressourcen

GEOBLOCKING UND IPS

Alex' Dilemma

BEWERTUNGSRICHTLINIE

Die Antworten der Schülerinnen und Schüler sollten folgende Punkte abdecken:

- Warum blockiert: Der Streaming-Anbieter nutzt Geoblocking, das die lokale IP-Adresse des Reisenden seinem tatsächlichen Aufenthaltsland zuordnet und sie aufgrund territorialer Lizenzen sperrt.
- Was funktioniert besser: Beide verschaffen ihm eine IP aus seinem Heimatland, aber ein Proxy deckt nur die konfigurierte App ab, während ein VPN zusätzlich den gesamten Datenverkehr seines Geräts verschlüsselt.