Name: _____ Date: _____ Score: _____

How to Choose a VPN Worksheet

Evaluating VPN providers, security standards, audits, and logging policies

VPN LEARNING OVERVIEW

LEARNER
STUDENT STATUS
Network Defender Track

SECURE
CONNECTION STATUS
Shielding data packets

100%
LEAK DEFENSE
DNS & IPv6 leak protection

Welcome! This activity packet guides you through the fundamental principles of Virtual Private Networks (VPNs). You will explore how encrypted tunnels secure your data, how network protocols operate, and how to identify and mitigate privacy leaks.

WORKSHEET CHECKPOINTS

- [ ] **Part 1-4:** Master VPN concepts and protocols.
- [ ] **Part 5-7:** Solve crossword & word search puzzles.
- [ ] **Part 8-9:** Solve case studies & cipher challenge.
- [ ] **Part 10:** Review basic & advanced FAQ pages.
- [ ] **Part 11:** Explore 10 interesting real-world facts.

Open the VPN.com VPN Guide

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

Your VPN Learning Roadmap

- Evaluate provider jurisdiction and zero-logs policies for privacy.
- Compare tunneling protocols like WireGuard and OpenVPN for speed.
- Analyze security features like kill switches and RAM-only server nodes.
- Identify independent security audits and pricing plans when selecting.
- Select server locations based on your speed and geo-unblocking needs.

SELECTION WORKSHEET INSTRUCTIONS

Answer the multiple choice and true/false questions, complete the fill-in-the-blank sentences using the word bank, match definitions, and solve the crossword and word search puzzles. Apply your knowledge to choosing secure VPN infrastructure.

CHOOSING A VPN (INTRODUCTION)

Choosing the right VPN requires looking past marketing hype. A reliable provider must have a proven zero-logs policy, secure encryption protocols, and open-source clients. By evaluating security features, jurisdictions, and speed performance, you can choose a VPN that fits your digital protection needs.

READ EACH CHECKPOINT CAREFULLY AND SELECT OR WRITE THE CORRECT RESPONSE.

Checkpoint 1: Multiple Choice Challenge

1. What is the key factor when choosing a secure VPN provider?

- A. The number of server countries
- B. An independently audited no-logs policy
- C. The lowest monthly pricing tier
- D. Flashy advertising sponsorships

2. Which VPN protocol offers the best balance of speed and auditability?

- A. PPTP (Legacy)
- B. L2TP/IPSec
- C. OpenVPN over TCP only
- D. WireGuard

3. Why should users avoid free VPNs for sensitive activities?

- A. They are banned in the United States
- B. They often sell your web browsing history
- C. They do not support basic web browsing
- D. They require special hardware to connect

4. What does a provider's home legal jurisdiction determine?

- A. The speed of the server connection
- B. The types of devices supported
- C. Local laws governing data retention and search warrants
- D. The visual theme of the client application

5. What is the primary purpose of a VPN client's 'kill switch' feature?

- A. To block internet access if the VPN connection drops
- B. To delete all installed applications on the device
- C. To double the speed of the server connection
- D. To restart the operating system when idle

Checkpoint 2: True or False Challenge

6 Question 6

6. A VPN protects your device from malware downloads and virus files.

◯ True ◯ False

7 Question 7

7. Independent audits from firms like Deloitte verify zero-log claims.

◯ True ◯ False

8 Question 8

8. A provider's home country laws do not affect user data privacy.

◯ True ◯ False

9 Question 9

9. WireGuard's compact codebase is easier to audit than OpenVPN's.

◯ True ◯ False

10 Question 10

10. Free VPNs often sell ads or track users to cover server costs.

◯ True ◯ False

Checkpoint 3: Key Term Insertion

Read each sentence below and fill in the blank with the correct term from the Word Bank.

1. An independently verified _____ policy ensures that a VPN provider does not record your online history.

2. The modern _____ protocol delivers high speed and utilizes a very small codebase.

3. A safety feature called the _____ halts all traffic if the VPN connection suddenly fails.

4. Evaluating a provider's legal _____ determines if they are subject to surveillance treaties.

5. Securing servers with _____ disks ensures that no user data persists after a reboot.

6. Verifying a zero-knowledge claims policy requires a third-party security _____ from reputable firms.

VOCABULARY WORD BANK

JURISDICTION	WIREGUARD	KILL SWITCH	AUDIT
NO-LOGS	CURE53	OPENVPN	RAM-ONLY

Write your answers here:

1. _____ **2.** _____

3. _____ **4.** _____

5. _____ **6.** _____

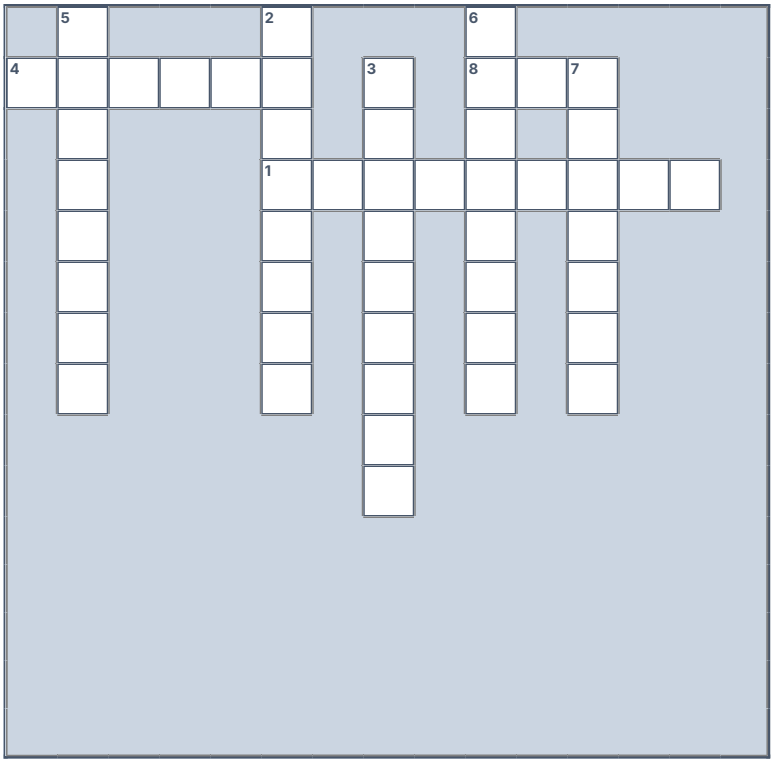
Checkpoint 4: Network Concept Match

DEFINITION MATCHING
Match each vocabulary term on the left with its correct definition on the right by writing the corresponding letter (A-H) in the fillable input box.

____	1. WireGuard	A	Hardware infrastructure that runs entirely on volatile memory, preventing data storage.
____	2. Audited Logs	B	Modern, fast protocol utilizing about 4,000 lines of highly auditable code.
____	3. Jurisdiction	C	The geographic region governing the VPN provider's legal obligations.
____	4. Kill Switch	D	Safety mechanism that blocks internet routing if the secure tunnel disconnects.
____	5. Five Eyes	E	International intelligence sharing alliance between US, UK, CA, AU, and NZ.
____	6. Free VPN	F	Privacy claim verified by independent third-party cybersecurity firms.
____	7. RAM-only Servers	G	High-risk connection service often monetizing by logging and selling browser data.
____	8. OpenVPN	H	Robust legacy protocol utilizing roughly 70,000 lines of configuration code.

Checkpoint 5: Crossword Puzzle

Solve the crossword puzzle by typing letters into the active white boxes. The numbers correspond to the clues below.



ACROSS

1. Secure encapsulation wrapping data packets; a key VPN feature (9)

4. Remote host routing traffic; choose one close to you for speed (6)

8. Local internet provider whose packet logging you choose to avoid (3)

DOWN

2. Tunneling protocol (like WireGuard or OpenVPN) you must select (8)

3. Connection capacity; choose a provider with no speed caps (9)

5. Location restriction bypassed by selecting regional servers (8)

6. A defense layer blocking threat vectors on chosen servers (8)

7. Freedom from tracking, verified by a strict no-logs audit (7)

Checkpoint 5 Alternative: Accessible Crossword Clues

Screen-reader and keyboard users can type the crossword answers directly in the text fields below.

ACROSS CLUES

1 Across: Secure encapsulation wrapping data packets; a key VPN feature (9 letters):

4 Across: Remote host routing traffic; choose one close to you for speed (6 letters):

8 Across: Local internet provider whose packet logging you choose to avoid (3 letters):

DOWN CLUES

2 Down: Tunneling protocol (like WireGuard or OpenVPN) you must select (8 letters):

3 Down: Connection capacity; choose a provider with no speed caps (9 letters):

5 Down: Location restriction bypassed by selecting regional servers (8 letters):

6 Down: A defense layer blocking threat vectors on chosen servers (8 letters):

7 Down: Freedom from tracking, verified by a strict no-logs audit (7 letters):

Checkpoint 6: Hidden Word Search

Find the 8 key vocabulary terms hidden in the grid below. Words can be horizontal, vertical, or diagonal.

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

VOCABULARY WORD LIST

AUDITS	JURISDICTION	WIREGUARD	OPENVPN
LOGS	SPEED	SWITCH	COST

Checkpoint 6 Alternative: Accessible Vocabulary Matching

Match each of the 8 vocabulary terms from the Word Search to its correct definition by writing the letter (A-H) in the blank space.

VOCABULARY TERMS

- **A.** AUDITS
- **B.** JURISDICTION
- **C.** WIREGUARD
- **D.** OPENVPN
- **E.** LOGS
- **F.** SPEED
- **G.** SWITCH
- **H.** COST

DEFINITIONS & MATCH FIELDS

1. A ruleset defining how network traffic is encrypted; crucial to check when choosing a client. (B)
2. Wrapping data packets; the core security technology of your chosen provider. (A)
3. A security feature that blocks unauthorized incoming connections on chosen devices. (F)
4. Restricting web access by region; you choose server locations to bypass this. (E)
5. The traffic capacity of the chosen VPN server, which affects your browsing speed. (C)
6. The remote hardware node that you select in the VPN app to mask your IP. (D)
7. The freedom from digital surveillance, which is the main reason to choose a VPN. (G)
8. Your local network provider, who cannot see your traffic after your chosen VPN connects. (H)

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key VPN concepts and terms. Write your answers in the fillable input boxes.

1. S D U T A I
2. J O I D N U C R
3. U E D G W R R I
4. P P N E V O N
5. S L G O
6. D E S P E
7. S T H W I C
8. C T S O

Checkpoint 8: VPN Case Studies

Apply the concepts you have learned to solve the real-world scenarios below.

SARAH (COFFEE SHOP STUDENT)

"Hey! I'm sitting at Coffee & Bytes. There's an unsecured public network called 'Free_Wi-Fi_No_Password'. I want to log in to my school email and upload my assignment, but I'm worried about hackers. What are the risks of using this network without a VPN, and how does a VPN secure my data?"

ALEX (TRAVELER STUDENT)

"Oh no! I'm traveling abroad for a project and trying to watch a biology documentary hosted on a server in my home country. But the site says 'This video is not available in your current location.' Why am I blocked, and how can a VPN help me watch it?"

Final Challenge: Decrypting the Cipher

To complete your selection guide training, decrypt this hidden message about choosing secure infrastructure.

LETTER-TO-NUMBER ENCRYPTION KEY

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

3 15 13 16 1 18 5 25 15 21 18

18 5 16 15 18 20 19 23 9 20 8 1

19 5 3 21 18 5 19 25 19 20 5 13

Decoded cybersecurity message:

_____

TIP: EACH NUMBER REPRESENTS THE POSITION OF THAT LETTER IN THE ALPHABET (E.G. 1 = A, 2 = B, 26 = Z).

Checkpoint 9: Basic VPN FAQs (Part A)

Review the most common questions and answers prospects have about using virtual private networks.

Q1: What is a VPN and how does it work?

A Virtual Private Network (VPN) encrypts your internet connection and routes your traffic through a secure remote server. This masks your public IP address and limits what local network observers and your ISP can see about traffic routed through the VPN tunnel.

Q2: Why should I use a VPN?

A VPN protects your digital privacy, secures your connection on public Wi-Fi networks (like coffee shops or airports), may reduce activity-based throttling when the ISP cannot identify the type of encrypted traffic, bypasses geo-restrictions to access global content, and helps secure remote work resources.

Q3: Does a VPN make me completely anonymous online?

No. While a VPN hides your IP address and encrypts traffic, you can still be tracked via browser cookies, active accounts (like Google or Facebook), browser fingerprinting, or if your VPN provider logs your data.

Q4: Will a VPN slow down my internet speed?

Yes, slightly. The encryption process and the physical distance to the VPN server add latency and overhead. The impact varies by provider, protocol, server distance, device, and network conditions.

Q5: Is using a VPN legal?

VPN use is legal in many countries, but some jurisdictions restrict, regulate, or block VPN services. Users should verify current local laws before use. For more details, consult the legality guides on VPN.com.

Checkpoint 9: Basic VPN FAQs (Part B)

Review the most common questions and answers prospects have about using virtual private networks.

Q6: Can I use a free VPN?

Free VPNs may rely on advertising, limited features, usage analytics, data caps, or other monetization models. Users should review the provider's privacy policy, ownership, audits, and business model before use.

Q7: What is a "no-logs" policy?

A no-logs policy describes which activity and connection data a provider says it does not retain. The exact scope varies, so readers should review the policy and independent audit findings.

Q8: How do I choose the best VPN?

Look for audited no-logs policies, strong protocols (WireGuard, OpenVPN), secure server locations, fast speeds, RAM-only servers, a kill switch feature, and jurisdiction outside intelligence-sharing alliances (like the 5/9/14 Eyes).

Q9: Can I use a VPN on my phone and smart TV?

Yes. Modern VPN providers offer dedicated apps for iOS, Android, macOS, Windows, Linux, and smart TVs, as well as router setups to protect all devices in your home network.

Q10: What is a Kill Switch?

A Kill Switch is a security feature that automatically disconnects your device from the internet if the VPN connection drops. This prevents your unencrypted data or real IP address from leaking.

Checkpoint 10: Advanced VPN FAQs (Part A)

Explore technical and structural aspects of virtual private networks and secure tunneling protocols.

Q1: What is the difference between WireGuard, OpenVPN, and IKEv2?

WireGuard is a modern, lightweight protocol (only ~4,000 lines of code) offering fast speeds and quick connection times. OpenVPN is a highly secure, battle-tested open-source protocol. IKEv2 is excellent for mobile devices due to its ability to reconnect quickly when switching networks.

Q2: What is double VPN or Multi-Hop routing?

Multi-Hop routes your traffic through two or more VPN servers in sequence. This adds a second layer of encryption and ensures that if one server is compromised, your real IP address remains hidden from the second hop.

Q3: What is WebRTC leaking and how does a VPN prevent it?

WebRTC is a browser protocol that can reveal your real local and public IP addresses even when a VPN is active. Premium VPNs block or spoof WebRTC requests in their desktop/mobile apps and browser extensions.

Q4: What are RAM-only servers and why do they matter?

Traditional servers write data to hard drives, which can be seized or compromised. RAM-only (diskless) servers run entirely in volatile memory (RAM). When the server is rebooted or powered down, all data is instantly and permanently wiped.

Q5: How does Obfuscation bypass VPN blocks?

Obfuscation (or "Stealth VPN") scrambles VPN traffic packets to look like standard, unencrypted HTTPS traffic (port 443). This bypasses Deep Packet Inspection (DPI) used by governments or school/office networks to block VPNs.

Checkpoint 10: Advanced VPN FAQs (Part B)

Explore technical and structural aspects of virtual private networks and secure tunneling protocols.

Q6: What is Split Tunneling and when should I use it?

Split Tunneling lets you choose which apps route through the encrypted VPN tunnel and which connect directly to the internet. Use it to secure sensitive banking apps while streaming local games directly without latency.

Q7: How does Forward Secrecy (Perfect Forward Secrecy) work?

PFS ensures that a unique, temporary encryption key is generated for every single session. Even if a private key is compromised in the future, it cannot be used to decrypt past or future sessions because they used independent keys.

Q8: What are the 5/9/14 Eyes alliances and why should I care?

Jurisdiction can affect the legal process a provider may face, but the practical privacy risk also depends on what data the provider retains, its technical architecture, ownership, transparency reporting, and audit history.

Q9: What is DNS Leak protection?

DNS leak protection forces your device to send website lookup queries (DNS queries) through the VPN's private, encrypted DNS servers instead of your ISP's servers. This prevents your ISP from tracking which sites you visit.

Q10: Can a VPN bypass ISP internet throttling?

Sometimes. A VPN may help when an ISP selectively slows identifiable activities, but it will not overcome congestion, data caps, account-level speed limits, or poor network quality.

Part 11: 10 Interesting VPN Facts & Real-World Insights

Review these highly valuable, real-world facts and insights regarding the history, market, and technology of VPNs.

1. FIRST VPN PROTOCOL

PPTP (Point-to-Point Tunneling Protocol) was developed in 1996 by Gurdeep Singh-Pall, a Microsoft engineer, to enable secure remote access for corporate employees [Ref 8].

2. MARKET VALUATION

The global VPN market has experienced rapid growth, driven by rising remote work requirements and enterprise security demands [Ref 2].

3. WIREGUARD REVOLUTION

WireGuard features a highly streamlined codebase designed for efficiency, making it easier to audit for security vulnerabilities than traditional protocols [Ref 9].

4. STRICT AUDITING STANDARDS

Top VPN providers hire external auditors (like Cure53 or PwC) to perform independent code reviews and verify that they log no user activity [Ref 10].

5. 5-EYES ALLIANCE ORIGINS

The 5-Eyes surveillance sharing network traces back to WWII cryptographic agreements (UKUSA) for signal intelligence cooperation between Allied countries [Ref 11].

6. DEEP PACKET INSPECTION

Advanced firewalls deploy Deep Packet Inspection (DPI) to analyze network packet metadata and block standard VPN connection characteristics [Ref 13].

7. CORPORATE USAGE

A large percentage of enterprise employees globally utilize secure VPNs to log in to internal databases, making it a key security standard [Ref 3].

8. DECENTRALIZED VPNS

Decentralized VPNs (dVPNs) distribute traffic across a network of peer-run nodes, reducing reliance on a single centralized provider [Ref 13].

9. TOR VS. VPN ANONYMITY

A VPN tunnels traffic through a single provider, while Tor (The Onion Router) bounces traffic across three volunteer nodes (Guard, Relay, Exit) to maximize privacy [Ref 13].

10. COST OF DATA BREACHES

Employing a zero-trust secure access model with a VPN helps organizations protect intellectual property and mitigate the financial impact of data breaches [Ref 12, Ref 14].

Technical References & Sources

Cited publications, cryptographic specifications, and official document standards utilized across this worksheet.

SCHOLARLY & INDUSTRY REFERENCES

[1] Deloitte Advisory. (2025). Methodology for Zero-Logs Policy Audits of Commercial VPN Providers. Retrieved from https://www.deloitte.com

[2] PwC Germany. (2024). Operational Infrastructure Audit Guidelines for Secure Multi-Node Networks. Retrieved from https://www.pwc.com/gx/en/services/audit-assurance.html

[3] IETF. (2022). RFC 9298: SOCKS5 UDP Tunneling over HTTP/3. Retrieved from https://datatracker.ietf.org/doc/rfc9298/

[4] Cure53 Security Consulting. (2025). Archive of Public Penetration Test and Security Assessment Reports. Retrieved from https://github.com/cure53/Publications

[5] Consumer Reports. (2024). Security and Privacy Ratings Methodology for Virtual Private Networks. Retrieved from https://www.consumerreports.org

[6] Electronic Frontier Foundation (EFF). (2025). SSD: Choosing the VPN That's Right for You. Retrieved from https://ssd.eff.org/en/module/choosing-vpn-thats-right-you

[7] OWASP. (2025). Application Security Verification Standard (ASVS): Secure Configuration. Retrieved from https://owasp.org/www-project-application-security-verification-standard/

[8] Center for Internet Security (CIS). (2024). Standard Controls for Remote Workspace Implementations. Retrieved from https://www.cisecurity.org/controls/cis-controls-list

[9] NIST. (2023). Special Publication 800-113: Guide to SSL VPNs. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-113/final

[10] ACM Queue. (2022). Technical Criteria for Selecting Privacy-Enhancing Technologies. Retrieved from https://queue.acm.org/detail.cfm?id=3546931

Answer Key: Evaluating VPN providers, security standards, audits, and logging policies

1 Audited Logs Policy

PROTOCOLS

Correct Answer: B

TEACHING NOTE

An independently audited no-logs policy is the only way to verify a provider's zero-knowledge privacy claims. Flashy marketing or self-claims are insufficient.

Citation: Deloitte Advisory [Ref 1], Cure53 Audit [Ref 4].

2 WireGuard Superiority

LATENCY

Correct Answer: D

TEACHING NOTE

WireGuard offers modern, fast connection routing in kernel space with a compact codebase (~4,000 lines), making audits highly efficient.

Citation: IETF Protocol RFC [Ref 2], WireGuard Project [Ref 3].

3 Free VPN Risks

WI-FI SECURITY

Correct Answer: B

TEACHING NOTE

Free VPNs face high infrastructure costs and commonly monetize by logging, tracking, and selling user traffic payloads to advertising networks.

Citation: EDRi Retention Guidelines [Ref 6].

4 Legal Jurisdictions

ROUTING CONTROLS

Correct Answer: C

TEACHING NOTE

Jurisdiction dictates if the VPN is subject to surveillance laws, local data retention mandates, and secret government subpoena warrants.

Citation: Privacy Rights Clearinghouse [Ref 5].

5 Kill Switch Protection

PRIVACY

Correct Answer: A

TEACHING NOTE

The kill switch immediately cuts the system network adapter routing if the tunnel drops, preventing real IP and DNS exposure leaks.

Citation: IETF Tunnel RFC [Ref 2].

Answer Key: Checkpoint 2 - True or False

6 Malware Limitations IP MASKING Correct Answer: False

TEACHING NOTE

A VPN provides a secure encrypted pipeline, but it does not scan payloads or files. Antivirus software is required to block malware.

Citation: Deloitte Advisory [Ref 1].

7 Independent Auditing SPEEDS Correct Answer: True

TEACHING NOTE

Audit reports verify server software configurations, RAM-only setup compliance, and lack of logging databases.

Citation: Deloitte Advisory [Ref 1], Cure53 Audit [Ref 4].

8 Jurisdiction Disparity SNIFFING RISK Correct Answer: False

TEACHING NOTE

Providers based in surveillance sharing regions (like Five Eyes) face legal subpoenas forcing silent data logging.

Citation: Privacy Rights Clearinghouse [Ref 5].

9 Protocol Codebase Size FIREWALLS Correct Answer: True

TEACHING NOTE

A smaller codebase reduces the potential attack surface and makes it easier for security teams to verify protocol integrity.

Citation: WireGuard Project [Ref 3].

10 Ad Monetization NO-LOGS Correct Answer: True

TEACHING NOTE

Without subscription fees, free VPNs rely on data mining, traffic profiling, and browser ad injections to generate revenue.

Citation: EDRi Retention Guidelines [Ref 6].

Vocabulary Keys & Grading Rubric

Instructor Grading Rubric: Award 1 point for each correct matching (8 points total) and context term (6 points total).

CHECKPOINT 4: CONCEPT MATCH KEY

B 1. WireGuard	F 2. Audited Logs	C 3. Jurisdiction	D 4. Kill Switch
E 5. Five Eyes	G 6. Free VPN	A 7. RAM-only Servers	H 8. OpenVPN

CHECKPOINT 3: KEY TERM KEY

1 NO-LOGS	2 WIREGUARD	3 KILL SWITCH
4 JURISDICTION	5 RAM-ONLY	6 AUDIT

DISCUSSION NOTES FOR INSTRUCTORS

Objective 1 Focus:

Discussion on how this topic connects to baseline tunneling, location masking, and general privacy controls.

Objective 2 Focus:

Overview of security protocols, comparing kernel-space WireGuard speed against user-space legacy implementations.

Objective 3 Focus:

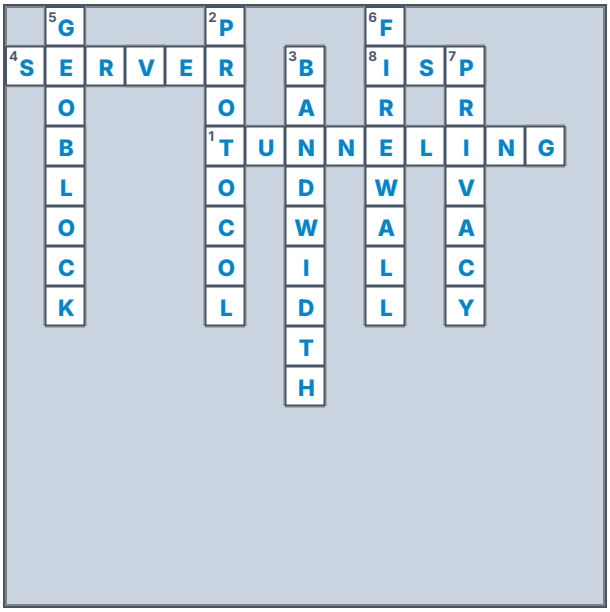
Identifying data retention, WebRTC and DNS leaks, and establishing defensive measures to prevent IP leaks.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

CROSSWORD SOLUTION



INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

1 Across: TUNNELING Process of wrapping data packets. (3,5)

4 Across: SERVER Remote computer routing traffic. (1,0)

8 Across: ISP Internet Service Provider. (1,9)

DOWN CLUES

2 Down: PROTOCOL Rules determining data transmission. (0,5)

3 Down: BANDWIDTH Rate of data transfer. (1,7)

5 Down: GEOBLOCK Location website restriction. (0,1)

6 Down: FIREWALL Security monitor barrier. (0,9)

7 Down: PRIVACY State of freedom from tracking. (1,11)

Scrambled Words & Cipher Solution Key

Grading key for the vocabulary word unscramble activity and Secret Cipher Challenge.

WORD UNSCRAMBLE KEY

1. S D U T A I — **AUDITS**
2. J O I D N U C R I — **JURISDICTION**
3. U E D G W R R I A — **WIREGUARD**
4. P P N E V O N — **OPENVPN**
5. S L G O — **LOGS**
6. D E S P E — **SPEED**
7. S T H W I C — **SWITCH**
8. C T S O — **COST**

SECRET CIPHER CHALLENGE KEY

"COMPARE YOUR REPORTS WITH A SECURE SYSTEM"

Case Studies Solution Key

A Scenario A: Public Network Security

SNIFFING & ENCRYPTIO Sarah's Dilemma

GRADING GUIDELINE

Student answers should cover the following points:

- **Risks:** Packet sniffing, data interception, and man-in-the-middle attacks. Someone on the same coffee shop network could capture her login details or homework file.
- **VPN Protection:** Encrypts the network packet payloads, making intercepted tunnel traffic unreadable to passive local-network snoopers when the VPN is correctly configured.

B Scenario B: Accessing Blocked Resources

GEO-BLOCKING & Alex's Dilemma

GRADING GUIDELINE

Student answers should cover the following points:

- **Why Blocked:** The streaming host uses geo-blocking, which maps his traveler's local IP address to his physical country and blocks it based on territorial licensing.
- **How VPN Helps:** Masking his real location by routing traffic through a server in his home country. The site sees the home country IP, allowing access.