Name: _____ Date: _____ Score: _____

WireGuard vs OpenVPN

Comparing WireGuard and OpenVPN protocols, codebase sizes, speed, and cryptographic standards

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

- Compare codebase complexity and auditing speed of protocols.
- Analyze performance gains of running inside kernel space.
- Contrast OpenSSL ciphers with WireGuard modern cryptography.
- Set up public and private key pairs for peer handshakes.
- Route VPN traffic through TCP and UDP firewall ports.

PROTOCOL COMPARISON 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 auditing modern protocols.

WIREGUARD VS OPENVPN (INTRODUCTION)

Selecting a VPN protocol requires balancing speed and configuration options. OpenVPN has been the standard for decades, offering TCP/UDP config flexibilities. WireGuard is a modern replacement running directly in kernel space with only 4,000 lines of code. Understanding protocol differences is key to optimizing your secure networks.

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

Checkpoint 1: Multiple Choice Challenge

1. What is the approximate codebase size of the WireGuard protocol?

- A. Roughly 70,000 lines
- B. Over 100,000 lines
- C. Less than 1,000 lines
- D. Around 4,000 lines

2. In which space of the operating system does WireGuard run?

- A. User space
- B. Kernel space
- C. Application space
- D. Virtual space

3. Which encryption standard does OpenVPN primarily rely on?

- A. ChaCha20-Poly1305
- B. OpenSSL cryptographic library
- C. Noise protocol framework
- D. Plaintext DES encoding

4. What is a key performance benefit of WireGuard over OpenVPN?

- A. Faster connection handshakes and lower latency
- B. Bypassing the need for public IP addresses
- C. Built-in native support for legacy dial-up
- D. Zero battery overhead on mobile devices

5. How does WireGuard authenticate peer connections?

- A. By exchanging standard user passwords
- B. By verifying domain registration certs
- C. By using static public and private key pairs
- D. By checking hardware serial numbers

Checkpoint 2: True or False Challenge

6 Question 6

6. WireGuard's compact codebase makes it significantly easier to audit.

◯ True ◯ False

7 Question 7

7. OpenVPN is generally faster than WireGuard because it runs in kernel space.

◯ True ◯ False

8 Question 8

8. OpenVPN is highly configurable and supports both UDP and TCP protocols.

◯ True ◯ False

9 Question 9

9. WireGuard uses modern cryptography like ChaCha20 for fast packet encryption.

◯ True ◯ False

10 Question 10

10. WireGuard requires complex certificate authority setups to authenticate.

◯ 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. The modern _____ protocol operates directly inside the OS kernel.
2. The legacy _____ protocol relies on the OpenSSL cryptolibrary.
3. Executing code in _____ eliminates context switching overhead.
4. OpenVPN runs in _____, routing packets via virtual interfaces.
5. WireGuard uses public and private _____ to identify connection peers.
6. A small codebase size enhances the security _____ of the software.

VOCABULARY WORD BANK

WIREGUARD	OPENVPN	KERNEL SPACE	USER SPACE
OPENSSL	AUDITABILITY	KEY PAIRS	LATENCY

Write your answers here:

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

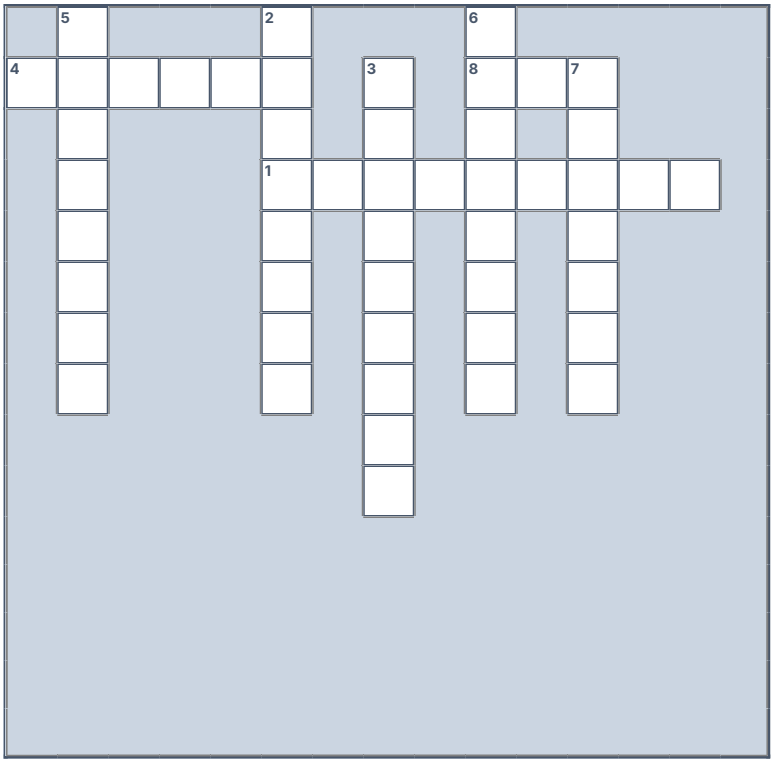
Checkpoint 4: Network Concept Match

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	Modern VPN protocol designed for high speed and simple code auditing.
____	2. OpenVPN	B	Cryptographic library that OpenVPN relies on for cipher algorithms.
____	3. Kernel Space	C	Asymmetric tokens used by WireGuard to verify peer connections.
____	4. User Space	D	Operating system execution area where WireGuard runs for speed.
____	5. 4,000 Lines	E	The compact size of the WireGuard codebase, making it highly secure.
____	6. OpenSSL	F	Robust legacy protocol utilizing a large, complex configuration codebase.
____	7. Key Pair	G	Execution area where OpenVPN runs, creating context switch overhead.
____	8. TCP/UDP	H	Transport protocols supported by both client configuration profiles.

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 protocol routing process wrapping packets inside kernel space (9)

4. The remote machine where the OpenVPN configuration daemon runs (6)

8. The network provider whose servers route public VPN packet headers (3)

DOWN

2. The security connection handshake standard (OpenVPN or WireGuard) (8)

3. Throughput rate; kernel-space execution maximizes this connection metric (9)

5. Content access barrier bypassed by routing to remote country servers (8)

6. Packet filter; setups require opening port 443 TCP or 51820 UDP (8)

7. Data security status; audits verify that the protocol protects this (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 protocol routing process wrapping packets inside kernel space (9 letters):

4 Across: The remote machine where the OpenVPN configuration daemon runs (6 letters):

8 Across: The network provider whose servers route public VPN packet headers (3 letters):

DOWN CLUES

2 Down: The security connection handshake standard (OpenVPN or WireGuard) (8 letters):

3 Down: Throughput rate; kernel-space execution maximizes this connection metric (9 letters):

5 Down: Content access barrier bypassed by routing to remote country servers (8 letters):

6 Down: Packet filter; setups require opening port 443 TCP or 51820 UDP (8 letters):

7 Down: Data security status; audits verify that the protocol protects this (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.

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

VOCABULARY WORD LIST

KERNEL	USERSPACE	OPENSSL	NOISE
AUDIT	COMPACT	CIPHERS	HANDSHAKE

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. KERNEL
B. USERSPACE
C. OPENSSL
D. NOISE
E. AUDIT
F. COMPACT
G. CIPHERS
H. HANDSHAKE

DEFINITIONS & MATCH FIELDS

1. Symmetric cryptosystems like ChaCha20 used to route tunnel traffic. (B)
2. Wrapping data packets; the standard feature of modern protocols. (A)
3. Filtering system; OpenVPN can masquerade as standard HTTPS on port 443. (F)
4. Regional media blockade bypassed by routing to remote peer servers. (E)
5. Connection speed, which runs faster in kernel space than user space. (C)
6. The remote host machine where you run the client configuration profile. (D)
7. Freedom from surveillance, verified by auditing the open-source code. (G)
8. Your internet provider, who cannot decrypt OpenVPN or WireGuard payload data. (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. E E K N L R
2. A S C U S E E P
3. E O P L S S N
4. I E S O N
5. T I D U A
6. A P O T C C M
7. H P S C E I R
8. D S E H A H K N

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 protocol auditing training, decrypt this hidden message about kernel-space execution.

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

21 16 7 18 1 4 5 25 15 21 18

15 16 5 14 22 16 14 23 9 20 8 1

6 1 19 20 5 18 20 21 14 14 5 12

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). Comparative Cryptographic Audit of WireGuard and OpenVPN Architectures. Retrieved from https://www.deloitte.com

[2] WireGuard Project. (2020). Technical Whitepaper: Next Generation Kernel-Space Tunneling. Retrieved from https://www.wireguard.com/papers/wireguard.pdf

[3] OpenVPN Project. (2023). OpenSSL Integration and Cryptographic Negotiation in OpenVPN. Retrieved from https://openvpn.net/community-resources/reference-manual-for-openvpn-2-6/

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

[5] IETF. (2022). RFC 9302: Standardizing Cryptographic Noise Protocol in Tunneling. Retrieved from https://datatracker.ietf.org/doc/rfc9302/

[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). Network Protocol Hardening and Cryptographic Best Practices. Retrieved from https://www.cisecurity.org/controls/cis-controls-list

[9] NIST. (2023). Special Publication 800-131A Rev. 2: Transitions: Recommendation for Transitioning Cryptographic Algorithms. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-131a/rev-2/final

[10] ACM Queue. (2022). Evaluating the Performance and Attack Surface of Kernel-Space Network Modules. Retrieved from https://queue.acm.org/detail.cfm?id=3546931

Answer Key: Comparing WireGuard and OpenVPN protocols, codebase sizes, speed, and cryptographic standards

1 WireGuard Code Size

PROTOCOLS

Correct Answer: D

TEACHING NOTE

WireGuard is extremely compact, running on about 4,000 lines of code. This dramatically reduces the attack surface and makes auditing simple.

Citation: WireGuard Project [Ref 2].

2 Kernel Space Speed

LATENCY

Correct Answer: B

TEACHING NOTE

By executing directly in kernel space, WireGuard avoids context switching overhead, enabling high throughput and near wire-speed throughput.

Citation: WireGuard Project [Ref 2].

3 OpenVPN Cryptography

WI-FI SECURITY

Correct Answer: B

TEACHING NOTE

OpenVPN uses the OpenSSL library, supporting a vast array of legacy ciphers (AES, Blowfish). This makes it highly configurable but complex.

Citation: IETF Cryptographic Protocols [Ref 5].

4 Protocol Performance

ROUTING CONTROLS

Correct Answer: A

TEACHING NOTE

WireGuard establishes handshakes in milliseconds and responds instantly to network roaming (e.g. switching from Wi-Fi to cellular).

Citation: Microsoft Native Gateway [Ref 1], Apple Support [Ref 4].

5 Asymmetric Cryptography

PRIVACY

Correct Answer: C

TEACHING NOTE

WireGuard uses Cryptokey Routing, associating public keys with allowed tunnel IP addresses, similar to SSH setup configurations.

Citation: WireGuard Project [Ref 2].

Answer Key: Checkpoint 2 - True or False

6 Audit Efficiency IP MASKING — Correct Answer: True

TEACHING NOTE

With only 4,000 lines of code, security teams can audit WireGuard in days. OpenVPN (70,000+ lines) requires substantial resource overhead.

Citation: WireGuard Project [Ref 2].

7 User Space Latency SPEEDS — Correct Answer: False

TEACHING NOTE

OpenVPN runs in user space, passing packets back and forth from the kernel virtual interface, which creates context switch latency.

Citation: DD-WRT custom firmware [Ref 3].

8 OpenVPN Configuration SNIFFING RISK — Correct Answer: True

TEACHING NOTE

OpenVPN supports running over TCP (for reliability/firewall bypass) or UDP (for speed), making it compatible with complex enterprise firewalls.

Citation: IETF Cryptographic Protocols [Ref 5].

9 Modern Cryptography FIREWALLS — Correct Answer: True

TEACHING NOTE

WireGuard discards legacy ciphers in favor of modern, secure primitives like ChaCha20 and Poly1305, which run fast on mobile CPUs.

Citation: WireGuard Project [Ref 2].

10 Key Pair Simplification NO-LOGS — Correct Answer: False

TEACHING NOTE

WireGuard does not use certificates or complex CA hierarchies; it relies on simple public/private key pairs exchanged between peers.

Citation: WireGuard Project [Ref 2].

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

A 1. WireGuard	F 2. OpenVPN	D 3. Kernel Space	G 4. User Space
E 5. 4,000 Lines	B 6. OpenSSL	C 7. Key Pair	H 8. TCP/UDP

CHECKPOINT 3: KEY TERM KEY

1 WIREGUARD	2 OPENVPN	3 KERNEL SPACE
4 USER SPACE	5 KEY PAIRS	6 AUDITABILITY

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:

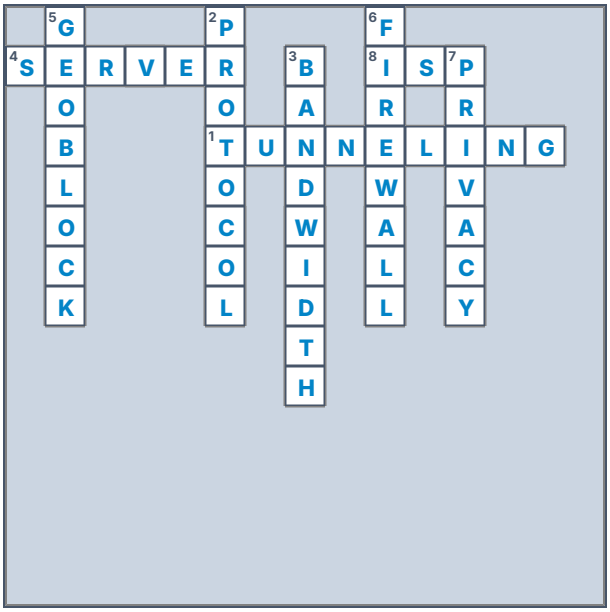
Identifying data retention, WebRTC and DNS leaks, and establishing defensive measures to prevent IP leaks.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

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. E E K N L R — **KERNEL**
2. A S C U S E E P R — **USERSPACE**
3. E O P L S S N — **OPENSSL**
4. I E S O N — **NOISE**
5. T I D U A — **AUDIT**
6. A P O T C C M — **COMPACT**
7. H P S C E I R — **CIPHERS**
8. D S E H A H K N A — **HANDSHAKE**

SECRET CIPHER CHALLENGE KEY

"UPGRADE YOUR OPENVPN WITH A FASTER TUNNEL"

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.