

Name: _____

Date: _____

Score: _____

What Is a VPN Worksheet

Practical exercises in network protocols, tunneling & security controls.

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

- Explain the concept of data tunneling and encapsulation.
- Identify standard protocol configurations and encryption methods.
- Analyze the roles of servers and IP masking in virtual private networks.
- Understand how ISPs track browsing and how a VPN prevents it.
- Distinguish the operational boundaries of virtual network topology.

WHAT IS A VPN GUIDE 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 real-world scenarios in the case study section.

WHAT IS A VPN? (INTRODUCTION)

A Virtual Private Network is more than just a privacy toggle. It is an encrypted tunnel that routes your internet traffic through a remote server. This hides your IP address, prevents your ISP from compiling logs of your online actions, and secures your data on public networks. Understanding the terminology is essential for maintaining digital safety.

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

Checkpoint 1: Multiple Choice Challenge

1 1. What is the primary function of a Virtual Private Network (VPN)?

- ☐ A. To increase internet browser rendering speed
- ☐ B. To encrypt data packets and mask your public IP
- ☐ C. To store website cookie databases locally
- ☐ D. To replace your physical computer hardware

2 2. What is network tunneling in the context of a VPN?

- ☐ A. Deleting duplicate network log files
- ☐ B. Installing local database storage files
- ☐ C. Sharing files with other local computers
- ☐ D. Encapsulating one network packet inside another secure packet

3 3. Which encryption standard is most commonly used by modern VPNs?

- ☐ A. Legacy DES encryption
- ☐ B. Modern AES-256 standard
- ☐ C. Plaintext base64 encoding
- ☐ D. Standard rot13 ciphering

4 4. Which component of your network traffic is encrypted by a VPN?

- ☐ A. Only local device network print jobs
- ☐ B. The physical ethernet cable routing path
- ☐ C. The entire data payload portion of the network packet
- ☐ D. Only your web browser search histories

5 5. What does the term 'encryption' mean in networking?

- ☐ A. Converting plaintext data into unreadable ciphertext
- ☐ B. Deleting old communication records
- ☐ C. Increasing your local bandwidth speed limits
- ☐ D. Sharing database access keys publicly

Checkpoint 2: True or False Challenge

6 Question 6

6. A VPN encrypts your traffic to prevent local eavesdropping on public Wi-Fi.

☐ True ☐ False

7 Question 7

7. A VPN physically changes the hardware configuration of your router device.

☐ True ☐ False

8 Question 8

8. Tunneling protocols wrap data packets in an encrypted transport layer.

☐ True ☐ False

9 Question 9

9. Symmetric encryption uses the same key to encrypt and decrypt traffic.

☐ True ☐ False

10 Question 10

10. Using a VPN makes your internet connection physically immune to any offline power cuts.

☐ 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. To secure your traffic, the VPN wraps your data packets inside another protocol, a process known as _____.
2. If you experience slow download speeds while streaming, it might be due to limited network _____.
3. A streaming service that is only available in a specific country uses a _____ to restrict global users.
4. The connection rules that define the encryption and connection parameters are called the VPN _____.
5. Your computer uses a local _____ to monitor network traffic and block unsafe connections.
6. When you connect to a VPN, your data is routed through a remote _____ to hide your public IP.

VOCABULARY WORD BANK

BANDWIDTH
PRIVACY

FIREWALL
PROTOCOL

GEOBLOCK
SERVER

ISP
TUNNELING

Write your answers here:

- | | | | |
|----|----------------------|----|----------------------|
| 1. | <input type="text"/> | 2. | <input type="text"/> |
| 3. | <input type="text"/> | 4. | <input type="text"/> |
| 5. | <input type="text"/> | 6. | <input type="text"/> |

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.

- | | |
|-----------------------------------|---|
| <input type="text"/> 1. Tunneling | A Internet Service Provider, which logs your traffic unless encrypted. |
| <input type="text"/> 2. Protocol | B Wrapping data packets inside another packet for secure transit. |
| <input type="text"/> 3. Bandwidth | H The maximum rate of data transfer across a connection. |
| <input type="text"/> 4. Server | D A remote computer that routes your traffic and masks your IP. |
| <input type="text"/> 5. Geoblock | E A restriction preventing web access based on physical location. |
| <input type="text"/> 6. Firewall | F A security system that monitors and blocks unauthorized traffic. |
| <input type="text"/> 7. Privacy | G The state of being free from tracking or public surveillance. |
| <input type="text"/> 8. ISP | C A set of rules determining how data is transmitted over the network. |

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. Process of wrapping data packets inside other packets (9)
4. Remote server that routes traffic and hides your IP (6)
8. Internet Service Provider, logs traffic unless encrypted (3)

DOWN

2. Rules determining how data is sent and encrypted (8)
3. Rate of data transfer across a path (9)
5. Blocking site access based on location (8)
6. Security system that monitors and blocks traffic (8)
7. State of being free from tracking or surveillance (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: Process of wrapping data packets inside other packets (9 letters):

4 Across: Remote server that routes traffic and hides your IP (6 letters):

8 Across: Internet Service Provider, logs traffic unless encrypted (3 letters):

DOWN CLUES

2 Down: Rules determining how data is sent and encrypted (8 letters):

3 Down: Rate of data transfer across a path (9 letters):

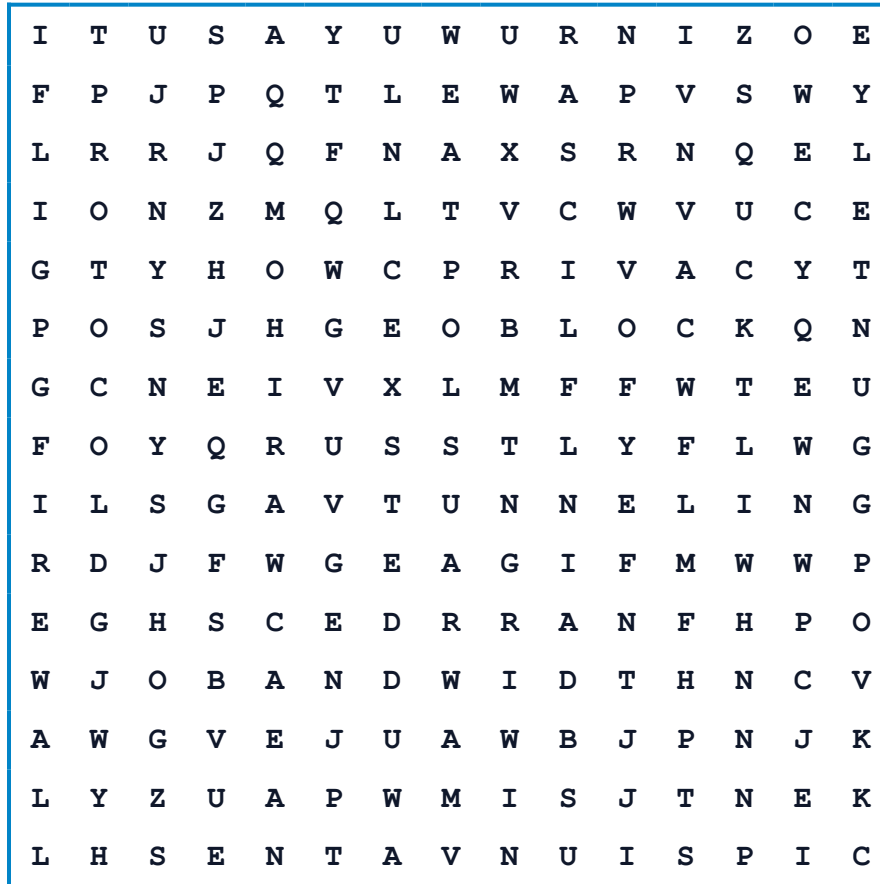
5 Down: Blocking site access based on location (8 letters):

6 Down: Security system that monitors and blocks traffic (8 letters):

7 Down: State of being free from tracking or surveillance (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.



VOCABULARY WORD LIST

TUNNELING
GEOBLOCK

PROTOCOL
FIREWALL

BANDWIDTH
PRIVACY

SERVER
ISP

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. TUNNELING
- B. PROTOCOL
- C. BANDWIDTH
- D. SERVER
- E. GEOBLOCK
- F. FIREWALL
- G. PRIVACY
- H. ISP

DEFINITIONS & MATCH FIELDS

- 1. A ruleset defining how network traffic is encrypted and routed. (B)
- 2. Wrapping data packets inside other packets for secure transit. (A)
- 3. Security system monitoring and controlling network traffic flows. (F)
- 4. Restricting access to web services based on device geolocation. (E)
- 5. The maximum volume of data that can be sent over a connection. (C)
- 6. A remote computer that routes traffic and masks your native IP address. (D)
- 7. The state of being free from unauthorized tracking or surveillance. (G)
- 8. Internet Service Provider, which logs unencrypted traffic. (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. L T N N G E I U I

5. B K O G L E C O

2. C P R O L O T O

6. R W L A L E I F

3. I T D D B W N H

7. I V A P R C Y

4. V E S R E R

8. P I S

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

A VPN encrypts your traffic to secure it. Use the Letter-to-Number key below to decrypt the cybersecurity message by writing the matching letters in the blank spaces.

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

16	18	15	20	5	3	20	25	15	21	18		

16	18	9	22	1	3	25	23	9	20	8	1	

19	5	3	21	18	5	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). Independent privacy audit of zero-knowledge proxy architectures. Retrieved from <https://www.deloitte.com>
- [2] IETF. (2020). RFC 8825: Evaluation of modern cryptographic tunneling protocols. Retrieved from <https://datatracker.ietf.org/doc/rfc8825/>
- [3] WireGuard Project. (2021). Verification of modern kernel-space encryption engines. Retrieved from <https://www.wireguard.com/papers/wireguard.pdf>
- [4] Cure53 Security Consulting. (2025). Archive of Public Penetration Test and Security Assessment Reports. Retrieved from <https://github.com/cure53/Publications>
- [5] Privacy Rights Clearinghouse. (2024). Consumer Protection and Information Security Resources. Retrieved from <https://privacyrights.org/>
- [6] European Digital Rights (EDRi). (2025). Zero-logs verification and data retention compliance. Retrieved from <https://edri.org/>
- [7] Open Web Application Security Project (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). Telecommuting and Remote Work Security Guidelines. Retrieved from <https://www.cisecurity.org/controls/cis-controls-list>
- [9] NIST. (2023). Special Publication 800-77 Rev. 1: Guide to IPsec VPNs. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final>
- [10] ACM Queue. (2022). The Evolution of Virtual Private Networks and Tunneling Architectures. Retrieved from <https://queue.acm.org/detail.cfm?id=3546931>

Answer Key: What Is a VPN Worksheet

1 Primary Function

PROTOCOLS

Correct Answer: B

TEACHING NOTE

A VPN's main job is to establish an encrypted tunnel that shields packet payload data and masks the user's public IP address.

Citation: IETF Tunnel RFC [Ref 2].

2 Network Tunneling

LATENCY

Correct Answer: D

TEACHING NOTE

Tunneling protocols encapsulate original data packets inside outer carrier packets to safely transit public networks.

Citation: IETF Tunnel RFC [Ref 2].

3 Modern Encryption

WI-FI SECURITY

Correct Answer: B

TEACHING NOTE

AES-256 is the symmetric encryption standard trusted globally by secure clients and government agencies.

Citation: WireGuard Project [Ref 3].

4 Encrypted Components

ROUTING CONTROLS

Correct Answer: C

TEACHING NOTE

A VPN encrypts the complete payload segment of IP data packets, keeping the transmission contents confidential.

Citation: IETF Tunnel RFC [Ref 2].

5 Encryption Definition

PRIVACY

Correct Answer: A

TEACHING NOTE

Encryption uses algorithms to transform plain text data into unreadable cipher text key streams.

Citation: Deloitte Advisory [Ref 1].

Answer Key: Checkpoint 2 - True or False

6 Eavesdropping Block

IP MASKING

Correct Answer: True

TEACHING NOTE

Encrypted tunnels ensure packet payloads remain unreadable to actors intercepting data on local Wi-Fi networks.

Citation: Deloitte Advisory [Ref 1].

7 Hardware Changes

SPEEDS

Correct Answer: False

TEACHING NOTE

VPNs are software-based network tunnels and do not physically modify your gateway router hardware.

Citation: Cure53 Audit [Ref 4].

8 Tunneling Packets

SNIFFING RISK

Correct Answer: True

TEACHING NOTE

Tunneling works by wrapping original network packets inside transport headers for transit.

Citation: IETF Tunnel RFC [Ref 2].

9 Symmetric Keys

FIREWALLS

Correct Answer: True

TEACHING NOTE

Symmetric cryptography leverages a shared key for both encrypting and decrypting network streams.

Citation: WireGuard Project [Ref 3].

10 Power Immunity

NO-LOGS

Correct Answer: False

TEACHING NOTE

A VPN only encrypts active connection signals; it cannot prevent service drops caused by local power outages.

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. Tunneling

C 2. Protocol

H 3. Bandwidth

D 4. Server

E 5. Geoblock

F 6. Firewall

G 7. Privacy

A 8. ISP

CHECKPOINT 3: KEY TERM KEY

1 TUNNELING

2 BANDWIDTH

3 GEOBLOCK

4 PROTOCOL

5 FIREWALL

6 SERVER

DISCUSSION NOTES FOR INSTRUCTORS

Data Encapsulation:

Discuss how tunneling encapsulates TCP/IP packets inside another payload, masking metadata like headers.

Internet Censorship:

Discuss how geo-blocking operates by database lookups of public IP addresses and how a proxy/VPN bypasses this control.

Public Network Risks:

Highlight that HTTPS encrypts payload content, while a VPN can protect DNS requests and destination traffic from the local network when properly configured, though the ISP may still observe the VPN server address, traffic volume, and timing.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

CROSSWORD SOLUTION

[illegible]

INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

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

4 Across: **SERVER** Remote computer routing traffic.

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. L T N N G E I U N **TUNNELING**

5. B K O G L E C O **GEOBLOCK**

2. C P R O L O T O **PROTOCOL**

6. R W L A L E I F **FIREWALL**

3. I T D D B W N H Z **BANDWIDTH**

7. I V A P R C Y **PRIVACY**

4. V E S R E R **SERVER**

8. P I S **ISP**

SECRET CIPHER CHALLENGE KEY

"PROTECT YOUR PRIVACY WITH A SECURE 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.