Name: _____ Date: _____ Score: _____

VPN.com VPN Guide Worksheet

Practical exercises in network protocols, tunneling & security controls.

VPN LEARNING OVERVIEW

LEARNER
STUDENT STATUS
Network Defender Track

SECURE
CONNECTION STATUS
Shielding data packets

ON
LEAK PROTECTION
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.**
- [ ] **Bonus: Think Fast challenge.**

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 bandwidth requirements.
- Analyze the roles of firewalls and geo-blocking in internet routing.
- Understand how ISPs track unencrypted browsing and how a VPN prevents it.
- Distinguish the operational boundaries of server location and jurisdiction.

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. Finish with the Bonus Activity: Think Fast.

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. What is a VPN protocol?

- A. A hardware device used to connect cables.
- B. A set of rules defining how data is encrypted and sent.
- C. A browser plugin that blocks advertisements.
- D. An internet service provider company.

2. If your VPN connection feels slow, what is the most likely cause?

- A. The VPN server is too far away or overloaded.
- B. Your monitor resolution is set too high.
- C. You have disabled web browser cookies.
- D. Your keyboard layout is configured incorrectly.

3. Why is a VPN highly recommended when connecting to public Wi-Fi?

- A. It makes the Wi-Fi connection free.
- B. It increases the range of the router.
- C. It encrypts traffic to block hackers on the same network.
- D. It deletes junk emails automatically.

4. Which of the following describes a geoblock?

- A. A tool that measures physical distance to a server.
- B. A restriction blocking site access based on location.
- C. A protocol for local file compression.
- D. A backup storage mechanism.

5. What can your Internet Service Provider (ISP) see when you use a VPN?

- A. Search keywords and web page content you view.
- B. That you are connected to a VPN, but not the traffic details.
- C. No information, not even that you are online.
- D. Your files and photos on your local hard drive.

Checkpoint 2: True or False Challenge

6 Location Masking

6. A VPN masks your device's public IP address, preventing third-party websites from easily identifying your physical location.

○ True ○ False

7 VPN Speed Impact

7. Enabling a VPN connection makes your baseline internet speed twice as fast as your connection without a VPN.

○ True ○ False

8 Public Wi-Fi Sniffing

8. If you use an unsecured public Wi-Fi network without a VPN, other users on that same network can potentially capture your unencrypted traffic.

○ True ○ False

9 Firewalls & Blocked Connections

9. Firewalls can be configured by network administrators to detect and block outgoing VPN connection tunnels.

○ True ○ False

10 Strict No-Logs Policies

10. A strict "no-logs" policy means that the VPN provider is legally required to store your search queries and visited links for at least 30 days.

○ 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 FIREWALL GEOBLOCK ISP PRIVACY PROTOCOL SERVER TUNNELING

Write your answers here:

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

Checkpoint 4: Network Concept Match

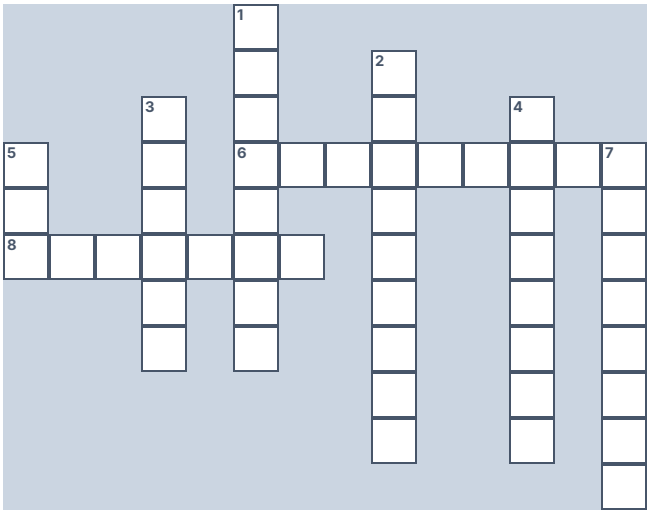
DEFINITION MATCHING

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. Tunneling	A	A set of rules determining how data is transmitted over the network.
☐	2. Protocol	B	The maximum rate of data transfer across a connection.
☐	3. Bandwidth	C	A restriction preventing web access based on physical location.
☐	4. Server	D	A security system that monitors and blocks unauthorized traffic.
☐	5. Geoblock	E	A remote computer that routes your traffic and masks your IP.
☐	6. Firewall	F	The state of being free from tracking or public surveillance.
☐	7. Privacy	G	Internet Service Provider that carries your traffic and can see unencrypted activity.
☐	8. ISP	H	Wrapping data packets inside another packet for secure transit.

Checkpoint 5: Crossword Puzzle

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



ACROSS CLUES

6. Wrapping data packets inside another packet for secure transit (9)

8. The state of being free from tracking or public surveillance (7)

DOWN CLUES

1. A set of rules determining how data is transmitted over the network (8)

2. The maximum rate of data transfer across a connection (9)

3. A remote computer that routes your traffic and masks your IP (6)

4. A security system that monitors and blocks unauthorized traffic (8)

5. Internet Service Provider that carries your traffic and can see unencrypted activity (3)

7. A restriction preventing web access based on physical location (8)

Checkpoint 5 Alternative: Accessible Crossword Clues

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

ACROSS CLUES

6 Across: Wrapping data packets inside another packet for secure transit (9 letters):

8 Across: The state of being free from tracking or public surveillance (7 letters):

DOWN CLUES

1 Down: A set of rules determining how data is transmitted over the network (8 letters):

2 Down: The maximum rate of data transfer across a connection (9 letters):

3 Down: A remote computer that routes your traffic and masks your IP (6 letters):

4 Down: A security system that monitors and blocks unauthorized traffic (8 letters):

5 Down: Internet Service Provider that carries your traffic and can see unencrypted activity (3 letters):

7 Down: A restriction preventing web access based on physical location (8 letters):

Checkpoint 6: Hidden Word Search

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

E T Z R J V L N Y E H S X Y F

X I U K J U G C P K R Z B D I

T V W G K M A E C G P Y F S O

Q D E N K V R O U Z Z T A S P

R J H V I E L U U C Z K F A M

T T Z R V B S L B A X Z L K X

U T P R O B S K M J R B I S P

N H E E E Q R T A E B S F M I

N S G D Q X C P R O T O C O L

E H T D I W D N A B P Y I E T

L W F O Y Q C R W D A P K L Q

I E C H P Q U O Z A X E W N F

N H W M A C M R W U B K V C X

G X I U Z F I R E W A L L T H

V B A J A D B D R F O M L U J

VOCABULARY WORD LIST

TUNNELING PROTOCOL BANDWIDTH SERVER GEOBLOCK FIREWALL PRIVACY 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. The state of being free from tracking or public surveillance.
2. A restriction preventing web access based on physical location.
3. A set of rules determining how data is transmitted over the network.
4. A security system that monitors and blocks unauthorized traffic.
5. The maximum rate of data transfer across a connection.
6. A remote computer that routes your traffic and masks your IP.
7. Internet Service Provider that carries your traffic and can see unencrypted activity.
8. Wrapping data packets inside another packet for secure transit.

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. LENUTINGN
2. HBTDAIDWN
3. BEGLOKCO
4. YRAVCPI
5. OCRLTPOO
6. EVSRRE
7. FLWALIER
8. PSI

Bonus Activity: Think Fast

3 ITEMS FROM EACH CATEGORY. FIRST PERSON TO COMPLETE THE LIST WINS.

1	Things you connect with the word 'tunnel'			
2	Things you'd teach your family about VPNs			
3	Things on a website that can track you			
4	Myths about VPNs			
5	Words from this worksheet you want to remember			
6	Devices that can use a VPN			
7	Things a VPN can't protect you from			
8	Countries you'd like to 'visit' online			
9	Promises a good VPN provider makes			
10	Ways to spot a fake Wi-Fi network			
11	Questions you have about VPNs			
12	VPN services you know			
13	Words related to privacy			
14	Things a VPN can hide			
15	Reasons to use a VPN at a café			

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?"

Checkpoint 9: Decrypting the Cipher

A VPN encrypts your traffic to secure it. Use the Letter-to-Number key below to decrypt the secret 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 message:

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

Checkpoint 10: 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 10: 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 C)

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. [3]

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 helps keep your real IP address hidden from the second hop if one server is compromised.

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, data held in memory is wiped.

Q5: How does Obfuscation bypass VPN blocks?

Obfuscation (or "Stealth VPN") disguises VPN traffic so it looks like ordinary HTTPS traffic (port 443). This can help it get past Deep Packet Inspection (DPI) used by governments or school/office networks to block VPNs.

Checkpoint 10: Advanced VPN FAQs (Part D)

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 route sensitive banking apps through the VPN while local games connect directly, avoiding VPN-added 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 by a vendor group including Microsoft and published as RFC 2637 in July 1999 to support remote-access VPNs. [6]

2. MARKET VALUATION

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

3. WIREGUARD REVOLUTION

WireGuard features a highly streamlined codebase designed for efficiency, making it easier to audit for security vulnerabilities than traditional protocols. [3]

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.

5. 5-EYES ALLIANCE ORIGINS

The Five Eyes alliance grew from the 1946 UKUSA signals-intelligence agreement between the US and UK, later joined by Canada, Australia and New Zealand.

6. DEEP PACKET INSPECTION

Deep Packet Inspection (DPI) examines packet contents and traffic patterns, not just headers, and some firewalls use it to detect and block common VPN protocols.

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.

8. DECENTRALIZED VPNS

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

9. TOR VS. VPN ANONYMITY

A VPN tunnels traffic through a single provider, while Tor (The Onion Router) sends traffic through three volunteer relays (guard, middle and exit) so no single relay knows both ends.

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.

Technical References & Sources

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

ACADEMIC LITERATURE & SECURITY STANDARDS

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

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

[3] Donenfeld, J. A. (2017). WireGuard: Next Generation Kernel Network Tunnel. NDSS Symposium.
https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/wireguard-next-generation-kernel-network-tunnel/

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

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

[6] IETF. (1999). RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
https://datatracker.ietf.org/doc/html/rfc2637

TECHNICAL STANDARDS SUMMARY

- Encapsulation Standards: RFC 4301 defines secure IPsec/L2TP internet packet routing.
- ISP Tracking: Routing DNS queries through the encrypted VPN tunnel can reduce DNS visibility to the local ISP.
- Firewall Control Protocols: Obfuscated stealth packets bypass deep packet filters.

Answer Key: Checkpoint 1 - Multiple Choice

1 Question 1

Correct Answer: B

TEACHING NOTE

A VPN protocol defines the rules for building the tunnel and encrypting data; the other options describe cables, ad blockers and ISPs.

2 Question 2

Correct Answer: A

TEACHING NOTE

Distance adds latency and an overloaded server has less capacity to share; screen resolution, cookies and keyboard layout do not affect connection speed.

3 Question 3

Correct Answer: C

TEACHING NOTE

On open networks others can intercept unencrypted packets; a VPN encrypts the traffic so intercepted data cannot be read.

4 Question 4

Correct Answer: B

TEACHING NOTE

Geo-blocking matches a visitor's public IP address to a location database and denies access outside permitted territories.

5 Question 5

Correct Answer: B

TEACHING NOTE

The ISP can see that you are sending encrypted data to a VPN server, but not which sites you visit or what you search.

Answer Key: Checkpoint 2 - True or False

6 Question 6

Correct Answer: True

TEACHING NOTE

Websites see the VPN server's IP address instead of yours, which hides your approximate location from them.

7 Question 7

Correct Answer: False

TEACHING NOTE

Encryption and the extra hop to the VPN server usually reduce speed slightly; a VPN cannot double your baseline connection speed.

8 Question 8

Correct Answer: True

TEACHING NOTE

On unsecured Wi-Fi, packet-sniffing tools can capture unencrypted traffic such as logins sent without HTTPS.

9 Question 9

Correct Answer: True

TEACHING NOTE

Administrators can block known VPN ports, such as OpenVPN's 1194, or use Deep Packet Inspection to detect VPN traffic.

10 Question 10

Correct Answer: False

TEACHING NOTE

A no-logs policy is a provider's promise not to keep records of your activity; no law requires VPNs to store searches for 30 days.

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

H 1. Tunneling	A 2. Protocol	B 3. Bandwidth	E 4. Server
C 5. Geoblock	D 6. Firewall	F 7. Privacy	G 8. ISP

CHECKPOINT 3: KEY TERM KEY

1 TUNNELING	2 BANDWIDTH	3 GEOBLOCK	4 PROTOCOL
5 FIREWALL	6 SERVER		

CHECKPOINT 6 ALTERNATIVE: VOCABULARY MATCH KEY

1 G – PRIVACY	2 E – GEOBLOCK	3 B – PROTOCOL	4 F – FIREWALL
5 C – BANDWIDTH	6 D – SERVER	7 H – ISP	8 A – TUNNELING

DISCUSSION NOTES FOR INSTRUCTORS

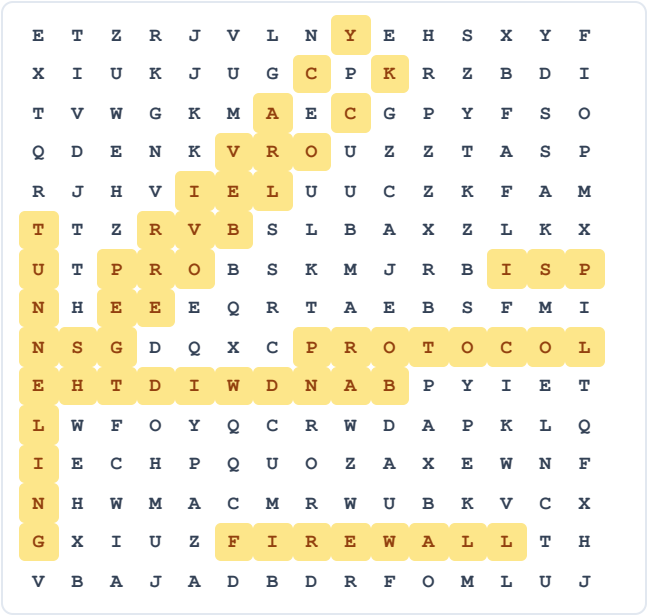
Key Terms:
Check that students can explain Tunneling, Protocol and Bandwidth in their own words and give an example of each.

Case Studies:
Ask students to support their recommendations with facts from the worksheet rather than assumptions.

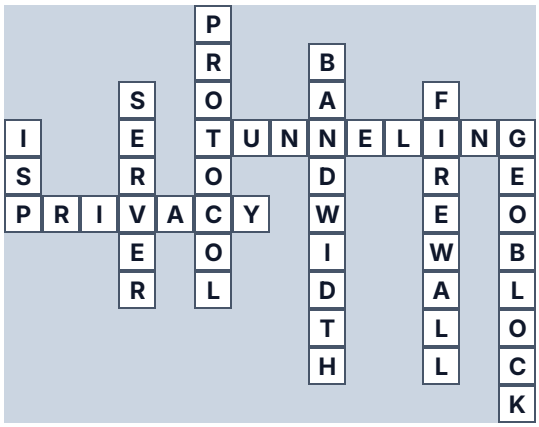
Source Evaluation:
Have students verify at least one claim against the worksheet references, and discuss why figures, prices and rules can change over time.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION



CROSSWORD SOLUTION



ACROSS CLUES

6 Across: TUNNELING Wrapping data packets inside another packet for secure transit (9 letters)

8 Across: PRIVACY The state of being free from tracking or public surveillance (7 letters)

DOWN CLUES

1 Down: PROTOCOL A set of rules determining how data is transmitted over the network (8 letters)

2 Down: BANDWIDTH The maximum rate of data transfer across a connection (9 letters)

3 Down: SERVER A remote computer that routes your traffic and masks your IP (6 letters)

4 Down: FIREWALL A security system that monitors and blocks unauthorized traffic (8 letters)

5 Down: ISP Internet Service Provider that carries your traffic and can see unencrypted activity (3 letters)

7 Down: GEOBLOCK A restriction preventing web access based on physical location (8 letters)

Scrambled Words & Cipher Solution Key

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

WORD UNSCRAMBLE KEY

1.	LENUTINGN	TUNNELING	5.	OCRLTPOO	PROTOCOL
2.	HBTDAIDWN	BANDWIDTH	6.	EVSRRE	SERVER
3.	BEGLOKCO	GEOBLOCK	7.	FLWALIER	FIREWALL
4.	YRAVCPI	PRIVACY	8.	PSI	ISP

SECRET CIPHER CHALLENGE KEY

"PROTECT YOUR PRIVACY WITH A SECURE TUNNEL"

Case Studies Solution Key

A Scenario A: Public Network Security

SNIFFING & ENCRYPTION | 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 & IPS | 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.