Name: _____ Date: _____ Score: _____

# Proxy vs VPN Worksheet

Comparing proxy servers and virtual private networks, encryption differences, and application vs system-wide routing

## 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

- Contrast application proxies with system-wide VPN encryption.
- Identify SOCKS5 capabilities compared to basic HTTP proxies.
- Analyze how browser-based proxies leave background apps exposed.
- Understand how ISPs log unencrypted traffic on proxy tunnels.
- Select the right routing tool based on speed and security needs.

## PROXY 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 comparing proxies and VPNs.

## PROXY VS VPN (INTRODUCTION)

Proxies and VPNs serve different digital privacy functions. A proxy server acts as an application-layer redirect, masking your IP address for specific programs without encrypting the data. A VPN operates at the network level, securing all system traffic with encryption. Choosing the right tool depends on your security requirements.

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

## Checkpoint 1: Multiple Choice Challenge

**1. At which layer of the OSI model does a standard HTTP proxy operate?**

- A. Physical layer
- B. Network layer
- C. Application layer
- D. Data Link layer

**2. What is a key protocol advantage of SOCKS5 over standard HTTP proxies?**

- A. It forces full payload encryption
- B. It supports any TCP/UDP traffic routing
- C. It is immune to DNS leaks
- D. It operates directly in kernel space

**3. Why is a VPN generally more secure than a proxy server?**

- A. It runs on faster remote hardware
- B. It encrypts all network traffic system-wide
- C. It does not require local routing tables
- D. It completely eliminates network latency

**4. Which proxy type redirects traffic without any encryption by default?**

- A. A basic HTTP proxy
- B. An encrypted HTTPS proxy
- C. A secure WireGuard client
- D. An obfuscated VPN server

**5. What happens to background application traffic when using a browser proxy?**

- A. It is encrypted automatically
- B. It is blocked by the proxy server
- C. It is routed through the proxy tunnel
- D. It bypasses the proxy and exposes your IP

## Checkpoint 2: True or False Challenge

### 6 Question 6

6. A SOCKS5 proxy encrypts all packet payloads going through the server.

◯ True ◯ False

### 7 Question 7

7. A VPN operates at the network layer to secure all system traffic.

◯ True ◯ False

### 8 Question 8

8. Proxies are generally faster than VPNs because they perform deep packet encryption.

◯ True ◯ False

### 9 Question 9

9. Configuring a proxy requires setting up traffic redirections inside specific apps.

◯ True ◯ False

### 10 Question 10

10. Using a proxy does not secure your data traffic from local ISP tracking.

◯ 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 application-layer _____ redirects specific browser traffic without securing other apps.
2. A robust _____ encapsulates and encrypts all device data packets.
3. The transport-layer _____ protocol handles both TCP and UDP data routing.
4. Proxies function at the _____ layer of the OSI model.
5. Standard proxy servers lack payload _____, leaving data vulnerable.
6. A VPN provides _____ protection for all network adapters.

**VOCABULARY WORD BANK**

| | | | |
|---|---|---|---|
| PROXY | VPN TUNNEL | SOCKS5 | APPLICATION |
| ENCRYPTION | SYSTEM-WIDE | HTTP | LATENCY |

**Write your answers here:**

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

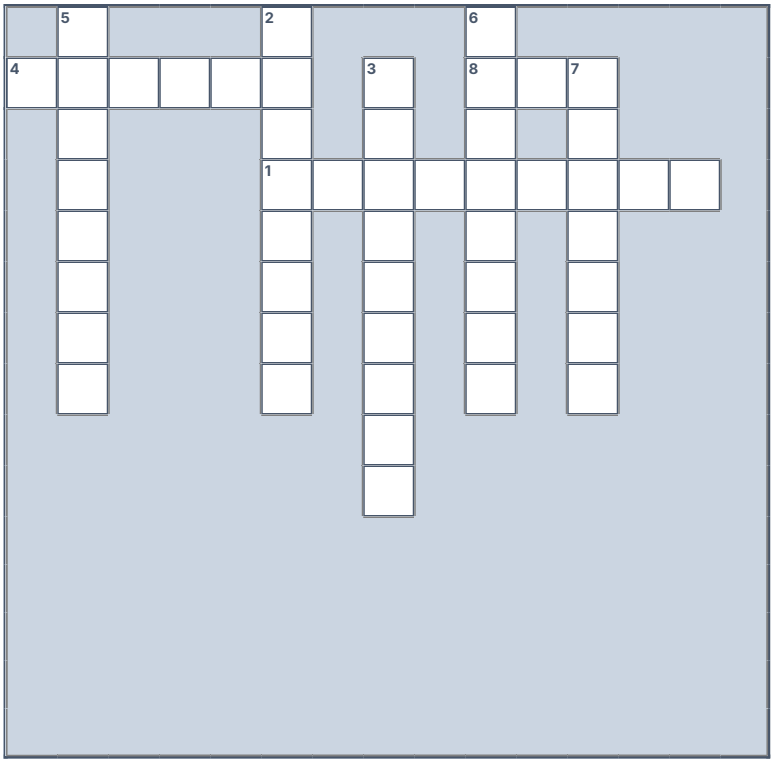
# Checkpoint 4: Network Concept Match

**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. HTTP Proxy | **A** Operating system level routing that encrypts all application traffic. |
| 2. SOCKS5 Proxy | **B** Application layer proxy redirecting specific web browser traffic. |
| 3. VPN Tunnel | **C** The Application layer where standard web proxy protocols operate. |
| 4. System-wide | **D** The capability of SOCKS5 to route any protocol, unlike HTTP proxies. |
| 5. OSI Layer 7 | **E** Protocol routing traffic at transport layer without encrypting data. |
| 6. UDP Support | **F** Traffic state where unencrypted proxy data remains visible to ISPs. |
| 7. Browser Proxy | **G** Client extension that only hides traffic inside the browser sandbox. |
| 8. ISP Visibility | **H** Encryption and encapsulation wrapping all background device traffic. |

## 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.** App-layer redirection of browser traffic; lacks system-wide security (9)

**4.** Intermediary host that routes browser traffic, acting as a gateway (6)

**8.** Internet provider that can track all unencrypted proxy connections (3)

### DOWN

**2.** Rules of communication used by the proxy (such as HTTP or SOCKS5) (8)

**3.** Data throughput; lack of payload encryption might increase this (9)

**5.** Regional restriction bypassed by selecting local proxy IPs (8)

**6.** Traffic filtration system; standard proxies bypass local rule checks (8)

**7.** Online anonymity status; not guaranteed by unencrypted HTTP proxies (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: App-layer redirection of browser traffic; lacks system-wide security (9 letters):**

**4 Across: Intermediary host that routes browser traffic, acting as a gateway (6 letters):**

**8 Across: Internet provider that can track all unencrypted proxy connections (3 letters):**

## DOWN CLUES

**2 Down: Rules of communication used by the proxy (such as HTTP or SOCKS5) (8 letters):**

**3 Down: Data throughput; lack of payload encryption might increase this (9 letters):**

**5 Down: Regional restriction bypassed by selecting local proxy IPs (8 letters):**

**6 Down: Traffic filtration system; standard proxies bypass local rule checks (8 letters):**

**7 Down: Online anonymity status; not guaranteed by unencrypted HTTP proxies (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.

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O | U | H | F | W | L | F | B | A | K | Y | Y | T | D | A |
| F | C | M | M | E | E | L | F | I | P | F | S | Z | Y | H |
| S | C | X | C | Y | B | L | A | P | V | A | N | Y | V | W |
| J | M | K | W | P | U | S | P | T | A | T | Y | C | Z | I |
| O | W | E | R | J | X | S | J | R | E | Y | G | J | N | J |
| U | R | A | J | S | C | U | H | H | N | N | L | E | A | A |
| X | Y | H | S | O | C | K | S | 5 | T | A | C | O | R | P |
| Y | L | T | S | B | R | B | F | B | B | T | V | Y | A | B |
| C | D | F | Y | Y | X | M | S | E | Y | R | P | N | A | D |
| S | U | E | S | P | E | P | X | N | D | J | H | S | C | I |
| D | H | E | T | A | K | S | A | S | O | M | B | Q | K | H |
| W | E | J | E | S | D | N | R | N | H | K | G | J | Z | R |
| T | Q | M | M | S | A | D | Q | A | K | D | Q | T | Y | C |
| O | H | T | T | P | T | G | W | L | I | R | S | J | H | W |
| I | A | V | S | P | J | T | R | A | F | F | I | C | K | L |

### VOCABULARY WORD LIST

| | | | |
|---|---|---|---|
| SOCKS5 | HTTP | HTTPS | LATENCY |
| BYPASS | SYSTEM | TRAFFIC | PAYLOAD |

# 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.** SOCKS5
**B.** HTTP
**C.** HTTPS
**D.** LATENCY
**E.** BYPASS
**F.** SYSTEM
**G.** TRAFFIC
**H.** PAYLOAD

**DEFINITIONS & MATCH FIELDS**

1. HTTP/SOCKS5 rulesets defining how proxy traffic is routed. (B)
2. Wrapping data packets inside a system-wide encrypted tunnel. (A)
3. System filtration that standard proxies bypass to route traffic. (F)
4. Blocking access to regional media hosts based on client location. (E)
5. The data capacity of SOCKS5 proxies that lack encryption overhead. (C)
6. The remote proxy server whose IP masks your browser destination. (D)
7. Digital anonymity, which unencrypted proxies fail to fully secure. (G)
8. Your local internet provider, who logs unencrypted proxy 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. S S 5 K C O

2. P T T H

3. S P T T H

4. A T E N Y C L

5. Y A P S S B

6. S S T M Y E

7. F R I A F T C

8. D O Y A P L A

## 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 proxy comparison training, decrypt this secret message about secure tunneling.

**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 |

18 5 18 15 21 20 5 25 15 21 18

20 18 1 6 6 9 3 23 9 20 8 1

19 15 3 11 19 -11 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). Performance and Security Comparison of Proxies and VPNs. Retrieved from https://www.deloitte.com

**[2]** IETF. (2021). RFC 1928: SOCKS Protocol Version 5 Specification. Retrieved from https://datatracker.ietf.org/doc/rfc1928/

**[3]** IETF. (2022). RFC 9301: LISP Control Plane Encapsulation and Routing. Retrieved from https://datatracker.ietf.org/doc/rfc9301/

**[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 Against Unencrypted Web Access. Retrieved from https://privacyrights.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). Deployment Guidelines for Secure Web Gateways and Proxies. Retrieved from https://www.cisecurity.org/controls/cis-controls-list

**[9]** NIST. (2023). Special Publication 800-125B: Secure Virtual Network Configuration for Virtual Proxies. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-125b/final

**[10]** ACM Queue. (2022). Network Latency and Protocol Overhead in Encrypted Tunnels vs Application Proxies. Retrieved from https://queue.acm.org/detail.cfm?id=3546931

# Answer Key: Comparing proxy servers and virtual private networks, encryption differences, and application vs system-wide routing

## 1 Proxy OSI Layer

PROTOCOLS

Correct Answer: C

### TEACHING NOTE

Standard HTTP/HTTPS proxies operate at the Application layer (Layer 7) and redirect specific browser traffic. They lack system-wide network routing.

Citation: Tor Project Foundation [Ref 1].

## 2 SOCKS5 Protocol

LATENCY

Correct Answer: B

### TEACHING NOTE

SOCKS5 handles any protocol (TCP/UDP) at the transport layer, but it does not perform encryption by default. HTTP proxies only handle web browser traffic.

Citation: IETF Proxy Vulnerabilities [Ref 3].

## 3 VPN System Encryption

WI-FI SECURITY

Correct Answer: B

### TEACHING NOTE

A VPN encapsulates and encrypts all operating system traffic system-wide, whereas a proxy only redirects traffic for specific configured applications.

Citation: Deloitte Advisory [Ref 1].

## 4 Proxy Encryption Lack

ROUTING CONTROLS

Correct Answer: A

### TEACHING NOTE

HTTP proxies forward browser traffic at the application layer without encrypting packet payloads, meaning your network operator or ISP can still trace your content traffic.

Citation: IETF Proxy Vulnerabilities [Ref 3].

## 5 Bypass Vulnerability

PRIVACY

Correct Answer: D

### TEACHING NOTE

Browser proxies only apply rules to the web browser itself. Background apps, operating system updates, and email clients bypass the proxy, exposing your native IP address.

Citation: W3C Consortium [Ref 2].

# Answer Key: Checkpoint 2 - True or False

**6 SOCKS5 Ciphering** IP MASKING — Correct Answer: False

### TEACHING NOTE

SOCKS5 redirects transport layer packets but performs no encryption by default. Any packet content remains readable in transit.

Citation: IETF Proxy Vulnerabilities [Ref 3].

**7 Network Layer Tunnels** SPEEDS — Correct Answer: True

### TEACHING NOTE

By running at the network layer, a VPN intercepts and encrypts all outbound traffic from your device, ensuring whole-system protection.

Citation: Deloitte Advisory [Ref 1].

**8 Proxy Encryption Limit** SNIFFING RISK — Correct Answer: False

### TEACHING NOTE

Proxies can sometimes be faster, but this is because they do NOT perform encryption. This lack of encryption leaves data vulnerable to inspection.

Citation: IETF Proxy Vulnerabilities [Ref 3].

**9 App-Level Redirection** FIREWALLS — Correct Answer: True

### TEACHING NOTE

Unlike system-wide VPNs, proxy servers require manual setup inside browser settings or application-specific proxy fields.

Citation: W3C Consortium [Ref 2].

**10 ISP Tracking Risk** NO-LOGS — Correct Answer: True

### TEACHING NOTE

Because standard HTTP/SOCKS5 proxies do not encrypt payload data, your local ISP retains full visibility of your online actions.

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. HTTP Proxy | E 2. SOCKS5 Proxy | H 3. VPN Tunnel | A 4. System-wide |
| C 5. OSI Layer 7 | D 6. UDP Support | G 7. Browser Proxy | F 8. ISP Visibility |

## CHECKPOINT 3: KEY TERM KEY

| | | |
|---|---|---|
| 1 PROXY | 2 VPN TUNNEL | 3 SOCKS5 |
| 4 APPLICATION | 5 ENCRYPTION | 6 SYSTEM-WIDE |

## 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:**

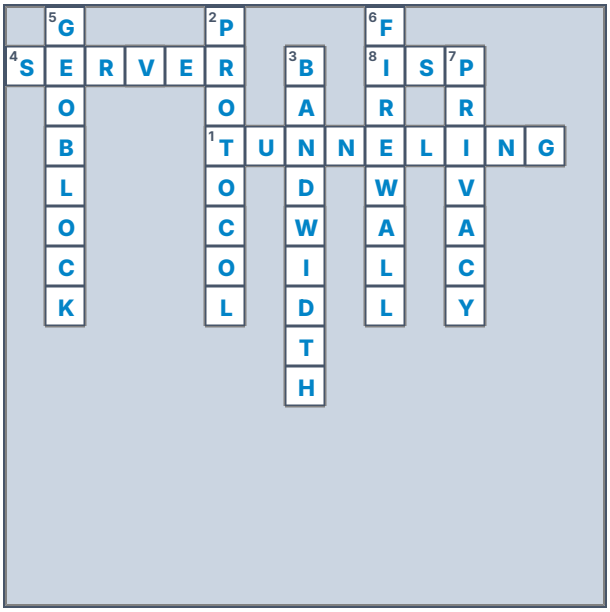
Identifying data retention, WebRTC and DNS leaks, and establishing defensive measures to prevent IP leaks.

# Puzzles Keys & Instructor Notes

## WORD SEARCH SOLUTION

| O | U | H | F | W | L | F | B | A | K | Y | Y | T | D | A |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F | C | M | M | E | E | L | F | I | P | F | S | Z | Y | H |
| S | C | X | C | Y | B | L | A | P | V | A | N | Y | V | W |
| J | M | K | W | P | U | S | P | T | A | T | Y | C | Z | I |
| O | W | E | R | J | X | S | J | R | E | Y | G | J | N | J |
| U | R | A | J | S | C | U | H | H | N | N | L | E | A | A |
| X | Y | H | S | O | C | K | S | 5 | T | A | C | O | R | P |
| Y | L | T | S | B | R | B | F | B | B | T | V | Y | A | B |
| C | D | F | Y | Y | X | M | S | E | Y | R | P | N | A | D |
| S | U | E | S | P | E | P | X | N | D | J | H | S | C | I |
| D | H | E | T | A | K | S | A | S | O | M | B | Q | K | H |
| W | E | J | E | S | D | N | R | N | H | K | G | J | Z | R |
| T | Q | M | M | S | A | D | Q | A | K | D | Q | T | Y | C |
| O | H | T | T | P | T | G | W | L | I | R | S | J | H | W |
| I | A | V | S | P | J | T | R | A | F | F | I | C | K | L |

## 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 S 5 K C O — **SOCKS5**
2. P T T H — **HTTP**
3. S P T T H — **HTTPS**
4. A T E N Y C L — **LATENCY**
5. Y A P S S B — **BYPASS**
6. S S T M Y E — **SYSTEM**
7. F R I A F T C — **TRAFFIC**
8. D O Y A P L A — **PAYLOAD**

**SECRET CIPHER CHALLENGE KEY**

**"REROUTE YOUR TRAFFIC WITH A SOCKS5 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.