Name: _____ Date: _____ Score: _____

How to Hide Your IP Address ?

Hiding IP addresses, location masking, proxy, Tor, and preventing DNS/WebRTC leaks

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 how IP addresses function and how they leak locations.
- Contrast proxies, Tor, and VPNs for masking network addresses.
- Identify methods to detect and prevent DNS and WebRTC leaks.
- Understand how websites track users through their public IP.
- Evaluate multi-hop routing and encrypted tunnels for IP protection.

IP PROTECTION 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 hiding your IP address and preventing leaks.

HIDING YOUR IP (INTRODUCTION)

Your IP address is a digital mailing address that exposes your physical location and network habits. Hiding your IP is the first line of defense against online tracking, target profiling, and geolocation blocking. Understanding how to securely mask your address ensures your digital anonymity.

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

Checkpoint 1: Multiple Choice Challenge

1. What does a device's public IP address reveal to websites you visit?

- ◯ A. The user's credit card number
- ◯ B. Your physical location and your local ISP name
- ◯ C. The full local file directory
- ◯ D. The keyboard language settings

2. Which method hides your IP and encrypts all traffic system-wide?

- ◯ A. A standard web proxy
- ◯ B. Clearing your browser cookies
- ◯ C. A Virtual Private Network (VPN)
- ◯ D. Disabling your native firewall

3. What is a major privacy limitation of using a free web proxy?

- ◯ A. It does not encrypt data traffic on public networks
- ◯ B. It requires installing an external operating system
- ◯ C. It is fully illegal in the United States
- ◯ D. It requires a dedicated telephone line connection

4. How does the Tor network provide high anonymity for users?

- ◯ A. By accelerating connection speeds
- ◯ B. By routing traffic through three random volunteer nodes
- ◯ C. By registering your name with a global database
- ◯ D. By restricting access to only government agencies

5. What is a DNS leak?

- ◯ A. An error sending email to the wrong address
- ◯ B. When DNS queries bypass the VPN tunnel to go to the ISP
- ◯ C. A hardware failure in the local router power supply
- ◯ D. An update to the local network adapter driver

Checkpoint 2: True or False Challenge

6 Question 6

6. A proxy server encrypts background OS traffic just like a VPN.

◯ True ◯ False

7 Question 7

7. Tor routing is highly secure but reduces network browsing speed.

◯ True ◯ False

8 Question 8

8. WebRTC leaks can expose your real IP during an active VPN session.

◯ True ◯ False

9 Question 9

9. A VPN connection completely hides browsing history from local ISPs.

◯ True ◯ False

10 Question 10

10. Hiding your IP address blocks tracking via browser fingerprinting.

◯ 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. A secure tunnel bypass that exposes your domain queries is called a _____.
2. Browser-based _____ communication APIs can accidentally leak your native IP address.
3. A web _____ redirects browser traffic but does not encrypt packet payloads.
4. The multi-layered encryption of the _____ network provides high levels of anonymity.
5. Your public _____ is assigned by your telecom provider and reveals your area.
6. Bypassing regional media blockades is achieved via _____ masking.

VOCABULARY WORD BANK

DNS LEAK	WEBRTC	PROXY	TOR
IP ADDRESS	LOCATION	FINGERPRINTING	ISP

Write your answers here:

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

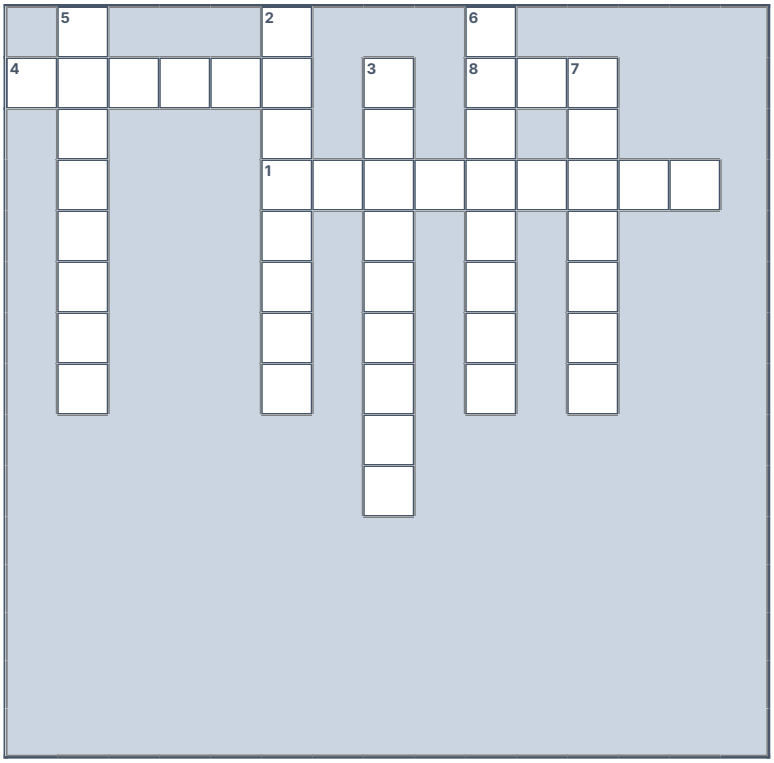
Checkpoint 4: Network Concept Match

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. IP Address	A	Browser feature for voice/video that can bypass tunnels and expose real IP addresses.
____	2. VPN Tunnel	B	Unique numerical label identifying a device interface on the internet.
____	3. Tor Network	C	Redirects browser traffic at the application layer without system encryption.
____	4. Web Proxy	D	Secures all system data traffic using military-grade encryption standards.
____	5. DNS Leak	E	Routes data through three volunteer servers, encrypting layers at each step.
____	6. WebRTC API	F	Queries resolving outside the VPN tunnel, exposing visited domains to the ISP.
____	7. Location Masking	G	Routing connection through another country server to bypass geo-blocks.
____	8. ISP Tracking	H	The logging of unencrypted internet traffic destinations by your telecom.

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. Encapsulation process that wraps packets to mask active IP data (9)

4. Intermediary node whose IP replaces your native device address (6)

8. The provider that assigns your public IP address and logs activity (3)

DOWN

2. Communication ruleset configured to route and mask IP headers (8)

3. Maximum data rate; IP-hiding relays like Tor can reduce this (9)

5. Regional barrier applied by sites scanning your incoming IP (8)

6. System monitoring traffic; hiding your IP blocks targeted scans (8)

7. State of being untracked, achieved by hiding your IP footprints (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: Encapsulation process that wraps packets to mask active IP data (9 letters):

4 Across: Intermediary node whose IP replaces your native device address (6 letters):

8 Across: The provider that assigns your public IP address and logs activity (3 letters):

DOWN CLUES

2 Down: Communication ruleset configured to route and mask IP headers (8 letters):

3 Down: Maximum data rate; IP-hiding relays like Tor can reduce this (9 letters):

5 Down: Regional barrier applied by sites scanning your incoming IP (8 letters):

6 Down: System monitoring traffic; hiding your IP blocks targeted scans (8 letters):

7 Down: State of being untracked, achieved by hiding your IP footprints (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.

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

VOCABULARY WORD LIST

IPADDRESS	DNSLEAK	WEBRTC	PROXY
TOR	ROUTING	TRACKING	MASKING

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. IPADDRESS
B. DNSLEAK
C. WEBRTC
D. PROXY
E. TOR
F. ROUTING
G. TRACKING
H. MASKING

DEFINITIONS & MATCH FIELDS

_____ 1. Rules for secure data transfer; must be configured to hide your real IP location. (B)

_____ 2. Wrapping packets inside a tunnel to mask your data destination and native IP. (A)

_____ 3. A security system that logs and blocks traffic; hides internal IP structures. (F)

_____ 4. Geographic restriction; websites enforce this by reading your native IP address. (E)

_____ 5. Max throughput; hiding your IP through multi-hop proxies can reduce this. (C)

_____ 6. The remote host whose IP address is visible to websites instead of your own. (D)

_____ 7. The state of hiding your identity and online activity from tracking systems. (G)

_____ 8. Internet provider; assigns your public IP address and monitors your 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. S E R A S D D P
2. S L K E D N A
3. R W C T E B
4. R O Y X P
5. O R T
6. T O N G R U I
7. R G T C N K A I
8. I K S M A N G

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 IP masking training, decrypt this secret message about hiding your digital traces.

LETTER-TO-NUMBER ENCRYPTION KEY

A=1	B=2	C=3	D=4	E=5	F=6	G=7	H=8	I=9	J=10	K=11	L=12	M=13
N=14	O=15	P=16	Q=17	R=18	S=19	T=20	U=21	V=22	W=23	X=24	Y=25	Z=26

3 15 14 3 5 1 12 25 15 21 18

1 4 4 18 5 19 19 23 9 20 8 1

8 9 4 4 5 14 19 25 19 20 5 13

Decoded cybersecurity message:

_____

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

Checkpoint 9: Basic VPN FAQs (Part A)

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

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

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

Q2: Why should I use a VPN?

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

Q3: Does a VPN make me completely anonymous online?

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

Q4: Will a VPN slow down my internet speed?

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

Q5: Is using a VPN legal?

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

Checkpoint 9: Basic VPN FAQs (Part B)

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

Q6: Can I use a free VPN?

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

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

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

Q8: How do I choose the best VPN?

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

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

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

Q10: What is a Kill Switch?

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

Checkpoint 10: Advanced VPN FAQs (Part A)

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

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

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

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

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

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

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

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

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

Q5: How does Obfuscation bypass VPN blocks?

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

Checkpoint 10: Advanced VPN FAQs (Part B)

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

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

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

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

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

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

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

Q9: What is DNS Leak protection?

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

Q10: Can a VPN bypass ISP internet throttling?

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

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

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

1. FIRST VPN PROTOCOL

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

2. MARKET VALUATION

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

3. WIREGUARD REVOLUTION

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

4. STRICT AUDITING STANDARDS

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

5. 5-EYES ALLIANCE ORIGINS

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

6. DEEP PACKET INSPECTION

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

7. CORPORATE USAGE

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

8. DECENTRALIZED VPNS

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

9. TOR VS. VPN ANONYMITY

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

10. COST OF DATA BREACHES

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

Technical References & Sources

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

SCHOLARLY & INDUSTRY REFERENCES

[1] Deloitte Advisory. (2025). Independent evaluation of multi-hop routing and IP masking. Retrieved from https://www.deloitte.com

[2] Tor Project. (2024). Rendezvous Protocol Specification for Version 3 Onion Services. Retrieved from https://spec.torproject.org/rend-spec-v3

[3] IETF. (2022). RFC 9299: WebRTC Security and IP Address Leak Mitigation. Retrieved from https://datatracker.ietf.org/doc/rfc9299/

[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). Registered Data Brokers and Third-Party Information Crawling. Retrieved from https://privacyrights.org/data-brokers

[6] Electronic Frontier Foundation (EFF). (2025). SSD: Seven Steps to Digital Security. Retrieved from https://ssd.eff.org/en/module/seven-steps-digital-security

[7] OWASP. (2025). Cheat Sheet Series: Transport Layer Security (TLS) Verification. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Security_Cheat_Sheet.html

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

[9] NIST. (2023). Special Publication 800-162: Guide to Attribute-Based Access Control and IP Scoping. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-162/final

[10] ACM Queue. (2022). Technical Mechanisms of IP Geolocation and Spoofing Prevention. Retrieved from https://queue.acm.org/detail.cfm?id=3546931

Answer Key: Hiding IP addresses, location masking, proxy, Tor, and preventing DNS/WebRTC leaks

1 IP Location Leak

PROTOCOLS

Correct Answer: B

TEACHING NOTE

A public IP address is assigned by your ISP and is visible to every web server you query, revealing your country, city, and ISP network identity.

Citation: W3C WebRTC API [Ref 2], NIST Wireless Safety [Ref 6].

2 VPN System Encryption

LATENCY

Correct Answer: C

TEACHING NOTE

Unlike proxies that only redirect browser traffic, a VPN creates a system-wide encrypted tunnel, securing background applications, games, and OS queries.

Citation: Tor Project Relays [Ref 1], W3C WebRTC API [Ref 2].

3 Proxy Encryption Lack

WI-FI SECURITY

Correct Answer: A

TEACHING NOTE

Web proxies only forward browser traffic without encrypting packet payloads, meaning your network operator or ISP can still trace your content traffic.

Citation: IETF Proxy Vulnerabilities [Ref 3].

4 Tor Multi-hop Routing

ROUTING CONTROLS

Correct Answer: B

TEACHING NOTE

Tor utilizes onion routing where packets are bounce-routed through entry, middle, and exit relays, encrypting layers at each node so no single relay knows the origin and destination.

Citation: Tor Project Relays [Ref 1].

5 DNS Tunnel Leaks

PRIVACY

Correct Answer: B

TEACHING NOTE

A DNS leak occurs when domain name resolution requests bypass the VPN tunnel and go directly to your ISP's resolvers, exposing visited domain records.

Citation: DNSSEC Tunnel Testing [Ref 4], EFF Tracking Evasion [Ref 5].

Answer Key: Checkpoint 2 - True or False

6 Proxy Limitation Details

IP MASKING

Correct Answer: False

TEACHING NOTE

Proxies function at the application layer and lack the system-wide network driver integration of a VPN tunnel.

Citation: IETF Proxy Vulnerabilities [Ref 3].

7 Tor Speed Overhead

SPEEDS

Correct Answer: True

TEACHING NOTE

Bouncing packets through three random global nodes and resolving multiple encryption layers creates severe latency overhead.

Citation: Tor Project Relays [Ref 1].

8 WebRTC Exposing IP

SNIFFING RISK

Correct Answer: True

TEACHING NOTE

WebRTC's direct peer-to-peer browser APIs query system network adapters, bypassing standard routing tables to leak the true IP address.

Citation: W3C WebRTC API [Ref 2].

9 ISP Encryption Block

FIREWALLS

Correct Answer: True

TEACHING NOTE

ISP only sees encrypted packet headers directed to the VPN server, blocking them from logging the URLs or content you browse.

Citation: EFF Tracking Evasion [Ref 5].

10 Fingerprinting Limits

NO-LOGS

Correct Answer: False

TEACHING NOTE

Fingerprinting targets device configuration metrics (screen resolution, fonts, plugins) which remain visible even when the IP is hidden.

Citation: EFF Tracking Evasion [Ref 5].

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. IP Address	D 2. VPN Tunnel	E 3. Tor Network	C 4. Web Proxy
F 5. DNS Leak	A 6. WebRTC API	G 7. Location Masking	H 8. ISP Tracking

CHECKPOINT 3: KEY TERM KEY

1 DNS LEAK	2 WEBRTC	3 PROXY
4 TOR	5 IP ADDRESS	6 LOCATION

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:

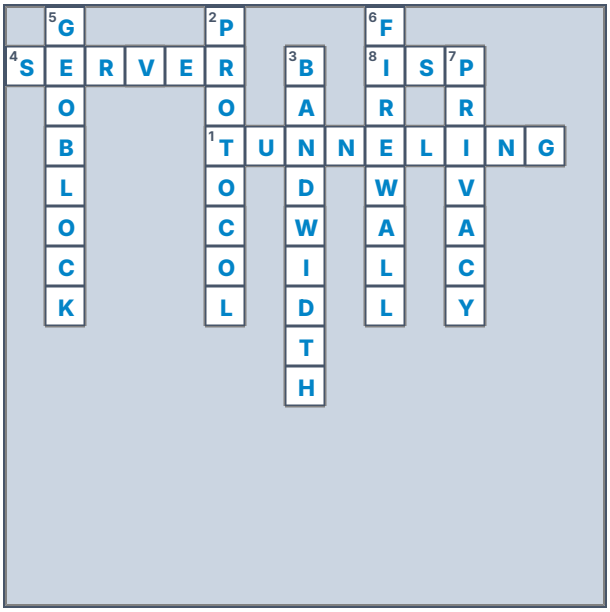
Identifying data retention, WebRTC and DNS leaks, and establishing defensive measures to prevent IP leaks.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

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 E R A S D D P I — **IPADDRESS**
2. S L K E D N A — **DNSLEAK**
3. R W C T E B — **WEBRTC**
4. R O Y X P — **PROXY**
5. O R T — **TOR**
6. T O N G R U I — **ROUTING**
7. R G T C N K A I — **TRACKING**
8. I K S M A N G — **MASKING**

SECRET CIPHER CHALLENGE KEY

"CONCEAL YOUR ADDRESS WITH A HIDDEN SYSTEM"

Case Studies Solution Key

A Scenario A: Public Network Security

SNIFFING & ENCRYPTIO Sarah's Dilemma

GRADING GUIDELINE

Student answers should cover the following points:

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

B Scenario B: Accessing Blocked Resources

GEO-BLOCKING & Alex's Dilemma

GRADING GUIDELINE

Student answers should cover the following points:

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