

Name: _____

Date: _____

Score: _____

Mozilla VPN Review

Technical analysis of US-headquartered Mozilla VPN, partnerships with Mullvad for RAM-only servers, high-speed WireGuard protocol, and open-source foundation principles.

MOZILLA VPN REVIEW 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 technical review of Mozilla VPN. You will explore Firefox Account integration, partnerships with Mullvad for RAM-only servers, and App Permissions split tunneling.

WORKSHEET CHECKPOINTS

- ☐ **Part 1-4:** Master VPN and network security configurations.
- ☐ **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 Best VPNs Guide

URL: <https://www.vpn.com/vpn/mozilla-vpn/>

Your Mozilla VPN Learning Roadmap

- Analyze the technical architecture and encryption standards of Mozilla VPN Review.
- Configure client settings to prevent IP, DNS, and WebRTC traffic leaks.
- Compare proprietary tunneling protocols against standard implementations.

MOZILLA VPN REVIEW 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 Mullvad partnerships and App Permissions.

CATAPULT HYDRA OPTIMIZATION & US JURISDICTION (INTRODUCTION)

Mozilla VPN is powered by Mullvad's server network and runs on the high-speed WireGuard protocol. It requires a Firefox Account to manage device access and benefits from open-source transparency, though it operates under US legal jurisdiction.

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

Checkpoint 1: Multiple Choice Challenge

1 What is the primary tunneling protocol used natively by Mozilla VPN?

- ☐ A) WireGuard
- ☐ B) OpenVPN
- ☐ C) SSTP
- ☐ D) L2TP/IPSec

2 Which provider's server network does Mozilla VPN lease to route user traffic?

- ☐ A) Mullvad
- ☐ B) NordVPN
- ☐ C) ExpressVPN
- ☐ D) IPVanish

3 Where is Mozilla, the parent organization of the VPN client, headquartered?

- ☐ A) United States
- ☐ B) Sweden
- ☐ C) Switzerland
- ☐ D) Germany

4 What account registry credential is required to sign up for Mozilla VPN?

- ☐ A) Firefox Account
- ☐ B) Google Account
- ☐ C) Proton Account
- ☐ D) Github Account

5 How many concurrent device connections are supported under a standard subscription?

- ☐ A) Five Devices
- ☐ B) Two Devices
- ☐ C) Unlimited
- ☐ D) Ten Devices

Checkpoint 2: True or False Challenge

6 Question 6

Mozilla VPN requires a Firefox Account registration to sign up and activate.

☐

True

☐

False

7 Question 7

Mozilla VPN owns and manages all of its physical server hardware globally.

☐

True

☐

False

8 Question 8

The client applications for Mozilla VPN are entirely open-source.

☐

True

☐

False

9 Question 9

Mozilla VPN includes a built-in split tunneling feature called App Permissions.

☐

True

☐

False

10 Question 10

Mozilla VPN operates its own custom transport protocol called Mimic.

☐

True

☐

False

Checkpoint 3: Key Term Insertion

Read each sentence below and fill in the blank with the correct term from the Word Bank.

1. The default connection tunnel is built on the fast _____ protocol.
2. Mozilla partners with _____ to utilize its global hosting servers.
3. To access the VPN, users must sign in with a registered _____ credentials.
4. Split tunneling is managed via the client feature called _____ selector.
5. The client apps are developed under an open and transparent _____ model.
6. Traffic is routed through an audited, multi-country _____ leased from partners.

VOCABULARY WORD BANK

WireGuard
Open Source

Mullvad
Server Network

Firefox Account
Kill Switch

App Permissions
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: VPN & Network Concept Match

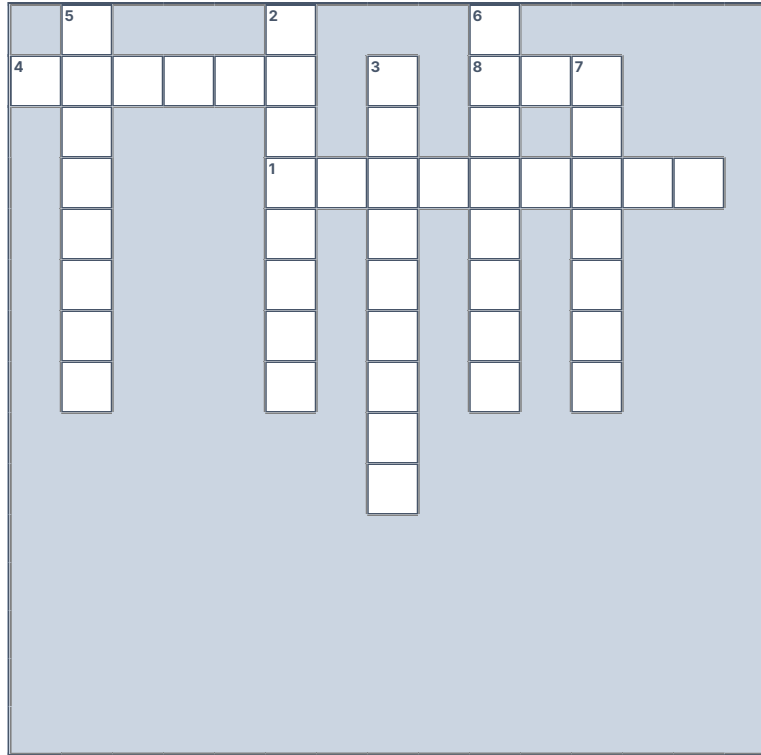
DEFINITION MATCHING

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"/> WireGuard | E Publicly readable client application source code files. |
| <input type="text"/> Mullvad | G Failsafe filter cutting connection on tunnel drop. |
| <input type="text"/> Firefox Account | D Split tunneling selector managing local software traffic. |
| <input type="text"/> App Permissions | B Partner server infrastructure routing client packets. |
| <input type="text"/> Open Source | A Modern high-performance open-source tunneling protocol. |
| <input type="text"/> Server Network | H Encapsulating data payloads across public networks. |
| <input type="text"/> Kill Switch | C Required user credential ID used to access service. |
| <input type="text"/> Tunneling | F Global array of servers leased to route user packets. |

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: Default open-source tunneling protocol. (9) (9 letters):

4 Across: Hosting server infrastructure partner. (7) (7 letters):

5 Across: Required user credentials account. (14) (7 letters):

7 Across: Split tunneling application selector. (14) (11 letters):

DOWN CLUES

2 Down: Publicly readable application source code. (10) (10 letters):

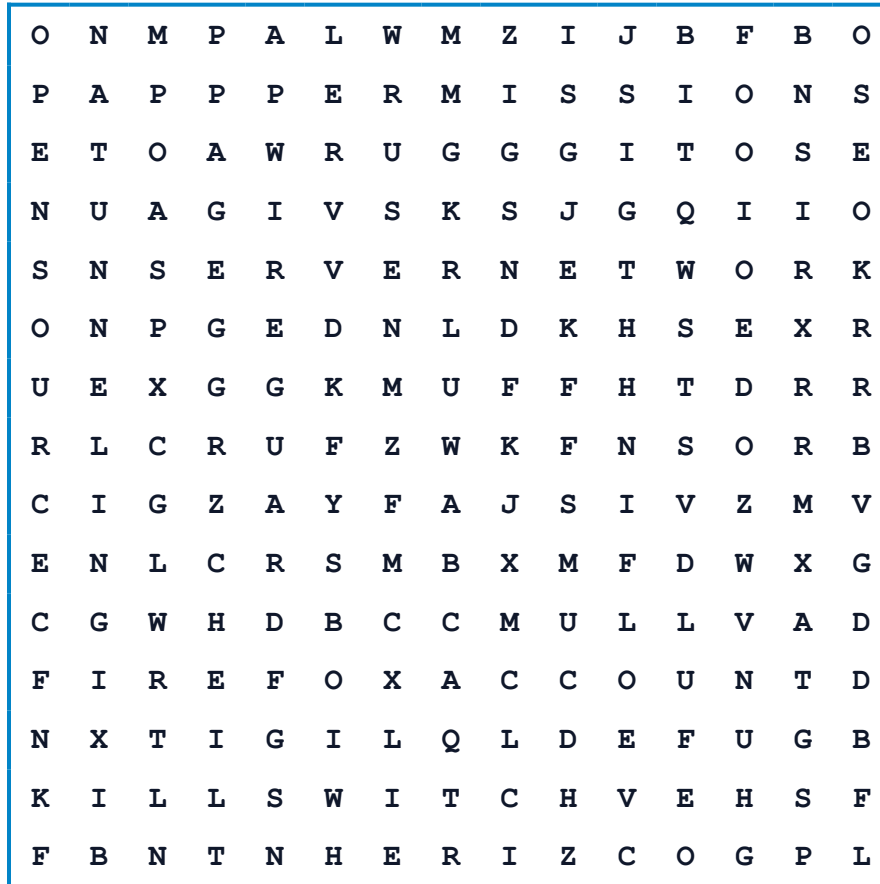
3 Down: Leased global server nodes group. (7) (7 letters):

6 Down: Failsafe traffic cutoff switch. (10) (10 letters):

8 Down: Encapsulating packet payloads on web. (8) (6 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

WireGuard
Open Source

Mullvad
Server Network

Firefox Account
Kill Switch

App Permissions
Tunneling

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. WireGuard
- B. Mullvad
- C. Firefox Account
- D. App Permissions
- E. Open Source
- F. Server Network
- G. Kill Switch
- H. Tunneling

DEFINITIONS & MATCH FIELDS

- 1. Modern high-performance open-source tunneling protocol.
- 2. Partner server infrastructure routing client packets.
- 3. Required user credential ID used to access service.
- 4. Split tunneling selector managing local software traffic.
- 5. Publicly readable client application source code files.
- 6. Global array of servers leased to route user packets.
- 7. Failsafe filter cutting connection on tunnel drop.
- 8. Encapsulating data payloads across public networks.

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key Virtual Private Network (VPN) concepts and terms. Write your answers in the input boxes provided.

1. IREGUARDW

5. PENSOURCEO

2. ULLVADM

6. ERVERSS

3. IREFOXF

7. ILLSWITCHK

4. ERMISIONSP

8. UNNELT

Checkpoint 8: VPN & Network Case Studies

Apply the concepts you have learned to solve the real-world scenarios below.



CASE STUDY 1: BROWSER-LEVEL TRAFFIC SECURITY

Scenario: A remote worker needs to secure their browser sessions on public networks using a simple, open-source VPN utility.

Discussion Question: Explain how Mozilla VPN leverages WireGuard and Open Source transparency to verify security for client browser data.



CASE STUDY 2: MANAGING MULTI-DEVICE LIMITS

Scenario: An administrator wants to secure 5 separate employee laptops using a single Mozilla VPN corporate subscription track.

Discussion Question: Describe the device configuration steps and explain what occurs when a sixth device attempts to connect to the account.

Final Challenge: Decrypting the Cipher

A network engineer secures routing channels and client tunnels. Use the Letter-to-Number key below to decrypt the 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

Decoded cybersecurity 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 regarding Virtual Private Networks (VPNs) and tunneling.

Q1: What protocol does Mozilla VPN use?

It uses the modern, lightweight WireGuard protocol as its default tunnel standard.

Q2: Does Mozilla VPN own its servers?

No, Mozilla leases its entire server network from Mullvad VPN, utilizing their diskless servers.

Q3: Are the Mozilla VPN client apps open-source?

Yes, all Mozilla VPN clients are open-source and hosted on GitHub for public review.

Q4: How many devices can I connect simultaneously?

A standard subscription allows up to 5 concurrent device connections under one account.

Q5: Is a Firefox Account required?

Yes, a Firefox Account is required to purchase, activate, and manage the VPN subscription.

Checkpoint 10: Basic VPN FAQs (Part B)

Review the most common questions and answers regarding Virtual Private Networks (VPNs) and tunneling.

Q6: Does Mozilla VPN support split tunneling?

Yes, its App Permissions feature allows split tunneling on Windows and Android clients.

Q7: Where is the parent organization based?

Mozilla Corporation is headquartered in the United States, operating under US jurisdiction.

Q8: Does the app include a kill switch?

Yes, it has a built-in, always-on firewall system that acts as a secure kill switch.

Q9: Can I pay for Mozilla VPN anonymously?

No, payments are handled via credit card or PayPal, which requires linking personal billing info.

Q10: Does Mozilla VPN work on routers?

No, Mozilla VPN does not currently support direct manual installation on router hardware.

Checkpoint 11: Advanced VPN FAQs (Part A)

Explore advanced technical aspects of VPN tunneling protocols, mobile client integrations, and enterprise deployment.

Q1: How does the partnership with Mullvad impact user logs?

Mozilla passes authentication tokens to Mullvad, but Mullvad's zero-logs policy prevents tracking of real IPs.

Q2: What encryption standard is used by WireGuard in the client?

It utilizes ChaCha20 symmetric encryption and Poly1305 authentication for high efficiency.

Q3: How does App Permissions handle background services?

It dynamically redirects network interfaces, routing chosen app packets through local gateway paths instead of the tunnel.

Q4: Are there privacy risks under US jurisdiction for Mozilla?

Yes, US agencies can issue subpoenas; however, the lack of activity logs protects browsing data from exposure.

Q5: Does Mozilla VPN support Multi-Hop routing?

Yes, premium clients support multi-hop routing, chaining two Mullvad server locations in series.

Checkpoint 11: Advanced VPN FAQs (Part B)

Explore advanced technical aspects of VPN tunneling protocols, mobile client integrations, and enterprise deployment.

Q6: How does the kill switch operate at the OS level?

It creates a persistent local system firewall block that intercepts all traffic during disconnects.

Q7: Does the VPN client protect against DNS leaks?

Yes, the client overrides system network adapters, routing all DNS queries to encrypted Mullvad DNS servers.

Q8: Does Mozilla VPN support IPv6 traffic natively?

Yes, the WireGuard implementation natively tunnels IPv6 traffic, preventing real IP leaks.

Q9: How has Mozilla verified its security posture?

Mozilla undergoes regular independent security audits of its client applications by firms like Cure53.

Q10: Does the client include ad and malware blockers?

Yes, the app has options to block ad networks, tracking scripts, and known malware domains.

Part 11: 10 Real-World VPN Facts & Insights

Review real-world facts regarding VPN encryption speeds, protocol audits, mobile connectivity, and enterprise remote work.

1. VPN INSIGHT

Mozilla VPN was launched in July 2020 as a paid service to diversify Mozilla's organizational revenues.

2. VPN INSIGHT

The client application is built using the Qt cross-platform framework for a unified UI across devices.

3. VPN INSIGHT

By leasing Mullvad's network, Mozilla VPN gains access to over 650 diskless, RAM-only servers globally.

4. VPN INSIGHT

All subscription revenues directly support Mozilla's non-profit foundation goals for a healthy internet.

5. VPN INSIGHT

The client automatically reconnects to the nearest server if it detects a network handshake drop.

6. VPN INSIGHT

Because it relies on Mullvad, its server distribution is concentrated in Europe and North America.

7. VPN INSIGHT

The client app has been audited multiple times by Cure53, resolving all high-severity bugs found.

8. VPN INSIGHT

Unlike Mullvad, Mozilla VPN does not accept cash payments or generate random account IDs.

9. VPN INSIGHT

WireGuard kernel modules are utilized on compatible Linux platforms to maximize connection throughput.

10. VPN INSIGHT

The client includes built-in protection against WebRTC IP leaks by masking local subnet details.

Technical References & Sources

The study guide and interactive puzzles are compiled from global technical standards, specifications, and regulatory frameworks.

SCHOLARLY & INDUSTRY REFERENCES

- [1] Mozilla. (2026). Mozilla VPN Security and Features Overview. Retrieved from <https://www.vpn.com/vpn/mozilla-vpn/>
- [2] Mozilla Support. (2026). How to Install Mozilla VPN on Windows and Mobile. Retrieved from <https://support.mozilla.org/en-US/products/firefox-private-network-vpn>
- [3] Mozilla Support. (2026). Firefox Account Authentication Details. Retrieved from <https://support.mozilla.org/en-US/products/firefox-private-network-vpn>
- [4] Mozilla Support. (2026). Managing Authorized Devices on Your Account. Retrieved from <https://support.mozilla.org/en-US/products/firefox-private-network-vpn>
- [5] Mozilla Support. (2026). Explaining App Permissions Split Tunneling. Retrieved from <https://support.mozilla.org/en-US/products/firefox-private-network-vpn>
- [6] Mozilla Support. (2026). Always-On Firewall and Kill Switch Settings. Retrieved from <https://support.mozilla.org/en-US/products/firefox-private-network-vpn>
- [7] Mozilla Support. (2026). Partner Infrastructure: Mullvad Server Network. Retrieved from <https://support.mozilla.org/en-US/products/firefox-private-network-vpn>
- [8] Mozilla Support. (2026). Security Audit Reports by Cure53. Retrieved from <https://support.mozilla.org/en-US/products/firefox-private-network-vpn>
- [9] Mozilla Support. (2026). Troubleshooting Speeds on WireGuard Tunnels. Retrieved from <https://support.mozilla.org/en-US/products/firefox-private-network-vpn>
- [10] VPN.com. (2026). Mozilla VPN Comprehensive Technical Review. Retrieved from <https://www.vpn.com/vpn/mozilla-vpn/>

Answer Key: Checkpoint 1 - Multiple Choice

1 Network Check 1

VPN PROTECTION

Correct Answer: A

TEACHING NOTE

What is the primary tunneling protocol used natively by Mozilla VPN?

Citation: IETF VPN RFC [Ref 3].

2 Network Check 2

VPN PROTECTION

Correct Answer: A

TEACHING NOTE

Which provider's server network does Mozilla VPN lease to route user traffic?

Citation: IETF VPN RFC [Ref 3].

3 Network Check 3

VPN PROTECTION

Correct Answer: A

TEACHING NOTE

Where is Mozilla, the parent organization of the VPN client, headquartered?

Citation: IETF VPN RFC [Ref 3].

4 Network Check 4

VPN PROTECTION

Correct Answer: A

TEACHING NOTE

What account registry credential is required to sign up for Mozilla VPN?

Citation: IETF VPN RFC [Ref 3].

5 Network Check 5

VPN PROTECTION

Correct Answer: A

TEACHING NOTE

How many concurrent device connections are supported under a standard subscription?

Citation: IETF VPN RFC [Ref 3].

Answer Key: Checkpoint 2 - True or False

6 Network Rule 1

VPN PROTECTION

Correct Answer: True

TEACHING NOTE

Mozilla VPN requires a Firefox Account registration to sign up and activate.

Citation: IETF VPN RFC [Ref 3].

7 Network Rule 2

VPN PROTECTION

Correct Answer: False

TEACHING NOTE

Mozilla VPN owns and manages all of its physical server hardware globally.

Citation: IETF VPN RFC [Ref 3].

8 Network Rule 3

VPN PROTECTION

Correct Answer: True

TEACHING NOTE

The client applications for Mozilla VPN are entirely open-source.

Citation: IETF VPN RFC [Ref 3].

9 Network Rule 4

VPN PROTECTION

Correct Answer: True

TEACHING NOTE

Mozilla VPN includes a built-in split tunneling feature called App Permissions.

Citation: IETF VPN RFC [Ref 3].

10 Network Rule 5

VPN PROTECTION

Correct Answer: False

TEACHING NOTE

Mozilla VPN operates its own custom transport protocol called Mimic.

Citation: IETF VPN RFC [Ref 3].

Vocabulary Keys & Grading Rubric

Instructor Grading Rubric: Award 1 point for each correct matching (8 points total) and context term (6 points total).

CHECKPOINT 4: CONCEPT MATCH KEY

A WireGuard

B Mullvad

C Firefox Account

D App Permissions

E Open Source

F Server Network

G Kill Switch

H Tunneling

CHECKPOINT 3: KEY TERM KEY

1 WireGuard

2 Mullvad

3 Firefox Account

4 App Permissions

5 Open Source

6 Server Network

DISCUSSION NOTES FOR INSTRUCTORS

Valuation Accuracy:

Verify that students understand how domain length, extension (.com, .ai), and commercial search volume drive appraisal pricing.

Escrow Security:

Emphasize that funds are held in licensed third-party holding accounts prior to domain WHOIS transfer verification.

Stealth Representation:

Highlight the role of NDAs and third-party representation in preventing speculative price gouging during corporate procurement.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

CROSSWORD SOLUTION

		5	G					2	P				6	F				
4	S	E	R	V	E	R				3	B			8	I	S	7	P
		O				O					A			R			R	
		B					1	T	U	N	N	E	L	I	N	G		
		L						O		D				W		V		
		O						C		W				A		A		
		C						O		I				L		C		
		K						L		D				L		Y		
										T								
										H								

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. IREGUARDW

WIREGUARD

5. PENSOURCEO

OPENSOURCE

2. ULLVADM

MULLVAD

6. ERVERSS

SERVERS

3. IREFOXF

FIREFOX

7. ILLSWITCHK

KILLSWITCH

4. ERMISIONSP

PERMISSIONS

8. UNNELT

TUNNEL

SECRET CIPHER CHALLENGE KEY

"MOZILLA VPN INTEGRATES FAST WIREGUARD ROUTING PROTOCOLS"

VPN & Network Case Studies Solution Key

A Case Study 1: Browser-Level Traffic Securi

[Instructor Solution](#)

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A remote worker needs to secure their browser sessions on public networks using a simple, open-source VPN utility.
- **Recommended Strategy & Solution:** Grading Guidance: Explain that WireGuard provides lightweight, fast kernel-level encryption, while open-source clients allow third-party auditing of the code.

B Case Study 2: Managing Multi-Device Limi

[Instructor Solution](#)

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** An administrator wants to secure 5 separate employee laptops using a single Mozilla VPN corporate subscription track.
- **Recommended Strategy & Solution:** Grading Guidance: Explain that the user must authorize devices via their Firefox Account, and a sixth device is blocked until an older device is deregistered.