

Name: _____

Date: _____

Score: _____

ProtonVPN Security

Analyzing ProtonVPN security architecture including Secure Core servers, NetShield DNS filtering, Swiss privacy jurisdiction, open-source audited apps, and Stealth protocol.

PROTONVPN SECURITY 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 Proton VPN's security architecture. You will explore Secure Core bunker servers, NetShield DNS blocking, Swiss privacy laws, and Stealth obfuscation.

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/protonvpn-security/>

Your ProtonVPN Security Learning Roadmap

- Analyze the technical architecture and configuration rules of ProtonVPN Security.
- Configure client settings to prevent IP, DNS, and WebRTC traffic leaks.
- Compare custom pricing, trial, and performance features against standard models.

PROTONVPN SECURITY 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 Secure Core bunker routing and Swiss privacy governance.

SECURE CORE BUNKER ARCHITECTURE & SWISS PRIVACY JURISDICTION (INTRODUCTION)

Proton VPN protects user traffic with Secure Core servers in Swiss underground bunkers, open-source audited applications, and the Stealth obfuscation protocol designed to bypass restrictive deep packet inspection.

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

Checkpoint 1: Multiple Choice Challenge

1 Where are Proton VPN's Secure Core servers housed?

- ☐ A) Commercial Cloud
- ☐ B) Underground Bunkers
- ☐ C) Public Data Centers
- ☐ D) Shared Racks

2 Which protocol helps bypass strict government censorship?

- ☐ A) PPTP
- ☐ B) Stealth Protocol
- ☐ C) OpenVPN UDP
- ☐ D) IKEv2

3 What is the function of Proton VPN's NetShield feature?

- ☐ A) Speed Booster
- ☐ B) DNS Ad & Malware Block
- ☐ C) Cloud Storage
- ☐ D) Port Forwarding

4 Under which country's privacy laws does Proton AG operate?

- ☐ A) United States
- ☐ B) United Kingdom
- ☐ C) Switzerland
- ☐ D) Panama

5 How are Proton VPN client applications verified by experts?

- ☐ A) Secret Code
- ☐ B) Open Source Audits
- ☐ C) Proprietary License
- ☐ D) Government Review

Checkpoint 2: True or False Challenge

6 Question 6

Secure Core routes traffic through privacy-friendly nations before exit.

☐ True ☐ False

7 Question 7

Switzerland is a member of the 14-Eyes intelligence surveillance alliance.

☐ True ☐ False

8 Question 8

NetShield blocks ads and malicious domains directly at the DNS level.

☐ True ☐ False

9 Question 9

Proton VPN applications are 100% open source and publicly audited.

☐ True ☐ False

10 Question 10

The Stealth protocol uses standard WireGuard headers without obfuscation.

☐ 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. Multi-hop traffic routing through hardened underground datacenters is called _____ architecture.
2. To defeat deep packet inspection and network firewalls, users activate _____ mode.
3. Malware domains, trackers, and advertising scripts are filtered by _____ DNS.
4. User privacy is protected under strict European data governance by _____ regulations.
5. If the VPN tunnel disconnects unexpectedly, internet traffic is blocked by the _____ guard.
6. Independent security researchers verify client integrity because apps are _____ code.

VOCABULARY WORD BANK

SECURECR
KILLSWCH

STEALTHP
OPENSRC

NETSHILD
WIREGURD

SWISSLWS
AES256GC

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.

SECURECR

B

An obfuscated tunneling protocol disguised as standard HTTPS web traffic.

STEALTHP

H

Military-grade symmetric cipher securing all encapsulated VPN data packets.

NETSHILD

G

A modern lightweight protocol providing robust cryptography and fast speeds.

SWISSLWS

C

A DNS-based filter blocking advertisements, telemetry trackers, and malware.

KILLSWCH

A

A multi-hop architecture routing traffic through hardened bunker servers.

OPENSRC

D

Strict legal privacy statutes in Switzerland outside 14-Eyes jurisdiction.

WIREGURD

F

Publicly accessible and independently audited client application software.

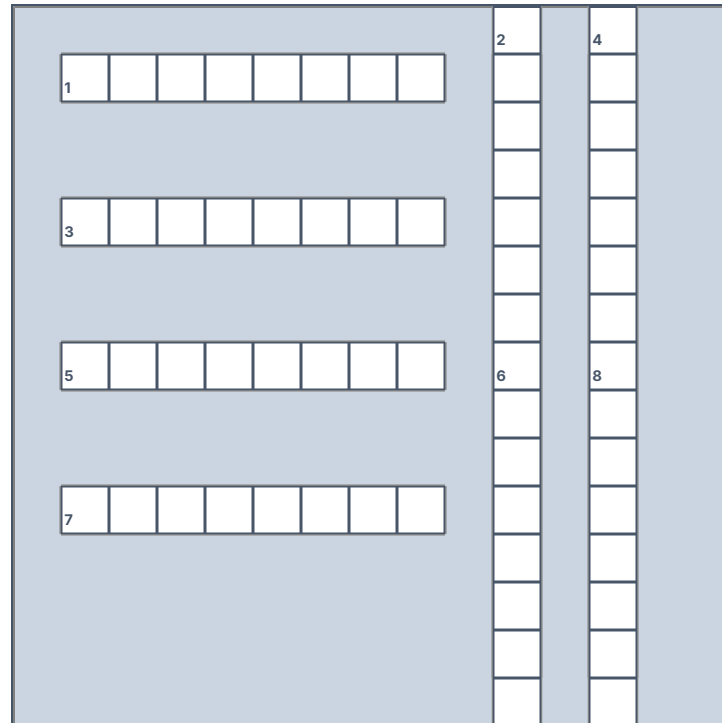
AES256GC

E

A security safeguard halting network transmission during connection drops.

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. Hardened multi-hop bunker server routing. (8 letters)
3. Obfuscation protocol bypassing restrictive firewalls. (8 letters)
5. DNS filter blocking trackers and malicious ads. (8 letters)
7. Strict non-EU legal privacy protections. (8 letters)

DOWN

2. Feature terminating network on tunnel disconnect. (8 letters)
4. Audited software transparent to the public. (8 letters)
6. Fast modern cryptographic tunneling protocol. (8 letters)
8. 256-bit Galois/Counter Mode encryption standard. (8 letters)

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: Hardened multi-hop bunker server routing. (8 letters):

3 Across: Obfuscation protocol bypassing restrictive firewalls. (8 letters):

5 Across: DNS filter blocking trackers and malicious ads. (8 letters):

7 Across: Strict non-EU legal privacy protections. (8 letters):

DOWN CLUES

2 Down: Feature terminating network on tunnel disconnect. (8 letters):

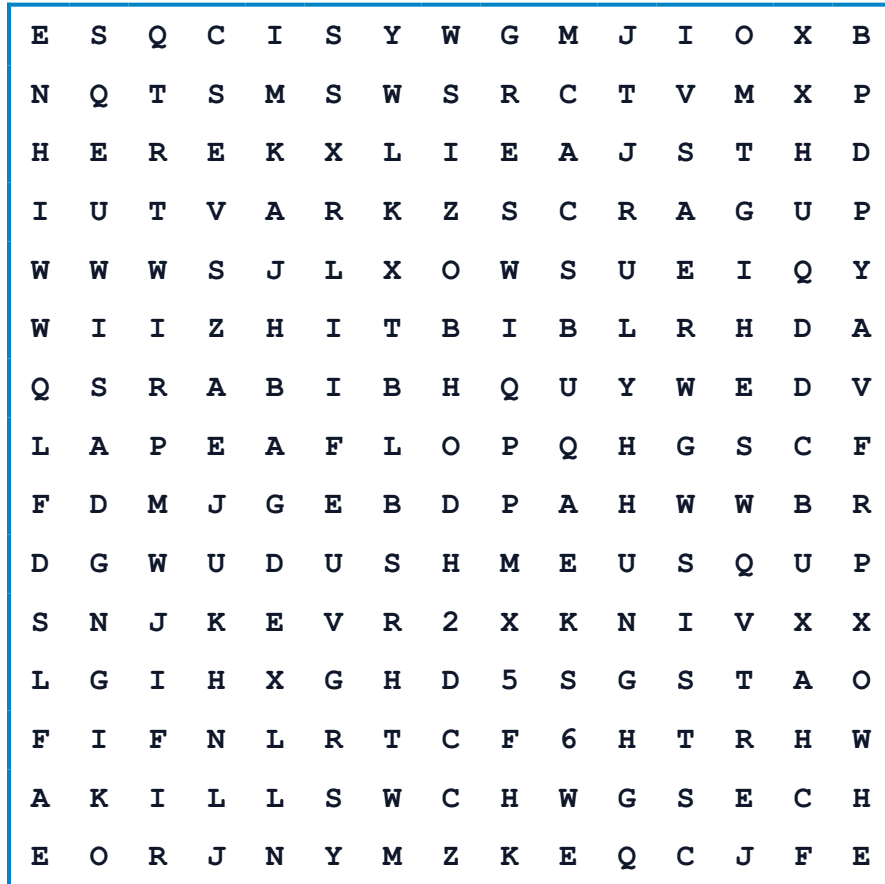
4 Down: Audited software transparent to the public. (8 letters):

6 Down: Fast modern cryptographic tunneling protocol. (8 letters):

8 Down: 256-bit Galois/Counter Mode encryption standard. (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.



VOCABULARY WORD LIST

SECURECR
KILLSWCH

STEALTHP
OPENSRC

NETSHILD
WIREGURD

SWISLWS
AES256GC

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. SECURECR
- B. STEALTHP
- C. NETSHILD
- D. SWISSLWS
- E. KILLSWCH
- F. OPENSRCR
- G. WIREGURD
- H. AES256GC

DEFINITIONS & MATCH FIELDS

- ☐ 1. A multi-hop architecture routing traffic through hardened bunker servers.
- ☐ 2. An obfuscated tunneling protocol disguised as standard HTTPS web traffic.
- ☐ 3. A DNS-based filter blocking advertisements, telemetry trackers, and malware.
- ☐ 4. Strict legal privacy statutes in Switzerland outside 14-Eyes jurisdiction.
- ☐ 5. A security safeguard halting network transmission during connection drops.
- ☐ 6. Publicly accessible and independently audited client application software.
- ☐ 7. A modern lightweight protocol providing robust cryptography and fast speeds.
- ☐ 8. Military-grade symmetric cipher securing all encapsulated VPN data packets.

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. ECURECRS

5. ILLSWCHK

2. TEALTHPS

6. PENSRCOE

3. ETSHILDN

7. IREGURDW

4. WISSLWSS

8. ES256GCA

Checkpoint 8: VPN & Network Case Studies

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



CASE STUDY 1: BYPASSING RESTRICTIVE FIREWALLS

Scenario: A user travels to a country where standard VPN traffic like OpenVPN and WireGuard is blocked by DPI.

Discussion Question: Which Proton VPN protocol configuration allows the user to bypass state-level inspection?



CASE STUDY 2: ADVANCED ADVERSARY PROTECTION

Scenario: A financial auditor suspects their local ISP exit node might be compromised by advanced persistent threats.

Discussion Question: How does Secure Core protect the auditor's identity against an exit node compromise?

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

19	5	3	21	18	5	3	15	18	5	8	1	18	4	5	14	5	4
19	5	18	22	5	18	19	16	18	15	20	5	3	20	21	19	5	18
4	1	20	1														

Decrypted Message Solution (Full Decoded Sentence):

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 is Proton VPN Secure Core?

Secure Core routes traffic through multiple servers in privacy-friendly nations before exit.

Q2: What is the Stealth protocol?

Stealth is an obfuscated protocol that hides VPN connections as regular TLS/HTTPS traffic.

Q3: How does NetShield protect users?

NetShield is a DNS-based tool that blocks ads, trackers, and malware domains automatically.

Q4: Is Proton VPN legally protected in Switzerland?

Yes, Switzerland has strict privacy laws and is outside US and EU/14-Eyes jurisdiction.

Q5: Are Proton VPN apps open source?

Yes, 100% of Proton VPN applications are open-source and undergo published security audits.

Checkpoint 10: Basic VPN FAQs (Part B)

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

Q6: What encryption ciphers are utilized?

Proton VPN uses AES-256-GCM or ChaCha20-Poly1305 with HMAC-SHA384 and RSA-4096 handshakes.

Q7: Does Proton VPN have a Kill Switch?

Yes, Proton VPN includes a standard and Permanent Kill Switch to prevent unencrypted leaks.

Q8: Can Proton VPN leak DNS queries?

No, all DNS queries are routed through encrypted private DNS servers owned by Proton.

Q9: Does Proton VPN keep connection logs?

No, Proton VPN adheres to a strict no-logs policy validated by independent SEC Consult audits.

Q10: Is Proton VPN vulnerable to WebRTC leaks?

No, Proton clients include built-in firewall rules and routing policies blocking WebRTC leaks.

Checkpoint 11: Advanced VPN FAQs (Part A)

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

Q1: Where are Secure Core data centers physically located?

Secure Core servers are located in a former Swiss military bunker and Iceland data facilities.

Q2: How does Perfect Forward Secrecy operate in Proton VPN?

A unique ephemeral encryption key is generated for every session, preventing retroactive decryption.

Q3: What is Permanent Kill Switch on Windows/Linux?

Permanent Kill Switch blocks all network traffic even if the VPN app is completely closed or crashes.

Q4: Does Proton VPN support IPv6 routing and leak defense?

Proton VPN fully routes IPv6 traffic through tunnels or safely disables it to prevent leaks.

Q5: How does NetShield DNS filtering handle HTTPS inspection?

NetShield operates purely at the DNS resolution layer without requiring invasive TLS decryption.

Checkpoint 11: Advanced VPN FAQs (Part B)

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

Q6: Who performed Proton VPN's third-party code audits?

Security audits are conducted by SEC Consult, Cure53, and other reputable cybersecurity firms.

Q7: How does Stealth protocol compare to OpenVPN XOR or Shadowsocks?

Stealth uses custom WireGuard TLS encapsulation, offering lighter overhead than OpenVPN XOR.

Q8: Can Swiss authorities compel Proton VPN to log traffic?

Under Swiss law, VPN services cannot be compelled to retain user activity or traffic metadata logs.

Q9: How are cryptographic public keys verified on client login?

Proton utilizes Key Transparency to cryptographically verify public keys across client devices.

Q10: Does Proton VPN support custom DNS server configurations?

Yes, paid subscribers can configure custom upstream DNS servers directly in app preferences.

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

1. Proton VPN's primary datacenter in Switzerland is housed in a high-security subterranean military bunker.

2. VPN INSIGHT

2. All Proton VPN client apps are 100% open-source and undergo recurring third-party code audits.

3. VPN INSIGHT

3. The Stealth obfuscation protocol bypasses Deep Packet Inspection by simulating standard TLS traffic.

4. VPN INSIGHT

4. Switzerland is outside the 5-Eyes, 9-Eyes, and 14-Eyes international intelligence sharing alliances.

5. VPN INSIGHT

5. NetShield operates at the DNS resolver level, preventing ads and malware before payload download.

6. VPN INSIGHT

6. Perfect Forward Secrecy ensures compromised keys cannot decrypt previously captured traffic sessions.

7. VPN INSIGHT

7. Proton VPN utilizes full-disk encryption on bare-metal servers to safeguard server configurations.

8. VPN INSIGHT

8. The Permanent Kill Switch prevents unencrypted data leaks even during operating system reboots.

9. VPN INSIGHT

9. SEC Consult has independently verified Proton VPN's no-logs policy across all infrastructure.

10. VPN INSIGHT

10. Proton VPN was developed by scientists who met at CERN (European Organization for Nuclear Research).

Technical References & Sources

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

SCHOLARLY & INDUSTRY REFERENCES

- [1] Proton AG. (2024). Proton VPN Security Architecture and Swiss Privacy Infrastructure. Proton Security Whitepaper. <https://protonvpn.com/features>
- [2] Proton AG. (2024). Proton VPN Subscription Plans, Account Billing, and Refund Policy. <https://protonvpn.com/pricing>
- [3] Securitum. (2023). Independent Security Audit Report: Proton VPN No-Logs Infrastructure & Architecture. Securitum Audit Services. <https://protonvpn.com/blog/no-logs-audit>
- [4] Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). Internet Engineering Task Force (IETF). <https://datatracker.ietf.org/doc/html/rfc8446>
- [5] Frankel, S., Hoffman, P., Orebaugh, A., & Park, R. (2020). Guide to IPsec VPNs (NIST Special Publication 800-77 Rev. 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-77r1>
- [6] Barker, E., & McKay, K. (2019). Guidelines for the Selection, Configuration, and Use of TLS Implementations (NIST SP 800-52 Rev. 2). NIST. <https://doi.org/10.6028/NIST.SP.800-52r2>
- [7] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., & Kivinen, T. (2014). Internet Key Exchange Protocol Version 2 (IKEv2) (RFC 7296). IETF. <https://datatracker.ietf.org/doc/html/rfc7296>
- [8] Electronic Frontier Foundation. (2024). Surveillance Self-Defense: Choosing the VPN That's Right for You. EFF. <https://ssd.eff.org/module/choosing-vpn-thats-right-you>

Answer Key: Checkpoint 1 - Multiple Choice

1 Secure Core Infrastructure

SECURE CORE

Correct Answer: B

TEACHING NOTE

Secure Core servers are housed in high-security underground military bunkers and former fallout shelters in Switzerland, Iceland, and Sweden.

Citation: Proton Physical Security [Ref 1].

2 Stealth Obfuscation Protocol

CENSORSHIP DEFENSE

Correct Answer: B

TEACHING NOTE

Proton's Stealth protocol disguises WireGuard connections as standard TLS/HTTPS traffic to bypass Deep Packet Inspection (DPI) firewalls.

Citation: Proton Stealth Protocol Whitepaper [Ref 2].

3 NetShield DNS Ad-Blocker

DNS FILTERING

Correct Answer: B

TEACHING NOTE

NetShield uses DNS-level filtering to block malware domains, spyware, intrusive advertising, and telemetry trackers before web pages load.

Citation: NetShield Security Specs [Ref 3].

4 Swiss Legal Jurisdiction

JURISDICTION

Correct Answer: C

TEACHING NOTE

Proton AG is headquartered in Geneva, Switzerland, benefiting from strong Swiss privacy laws outside US and EU 14-Eyes surveillance alliances.

Citation: Swiss Federal Data Protection Act [Ref 4].

5 Open Source Transparency

CODE AUDITS

Correct Answer: B

TEACHING NOTE

100% of Proton VPN client applications are open source on GitHub and undergo regular independent security audits by SEC Consult.

Citation: SEC Consult Audit Verification [Ref 5].

Answer Key: Checkpoint 2 - True or False

6 Secure Core Multi-Jurisdiction

ROUTING ARCHITECTURE

Correct Answer: True

TEACHING NOTE

Secure Core routes traffic through privacy-hardened jurisdictions before exiting to the destination country, neutralizing exit node compromise.

Citation: Secure Core Architecture [Ref 6].

7 Swiss Surveillance Alliance

SURVEILLANCE ALLIANCES

Correct Answer: False

TEACHING NOTE

Switzerland is not a member of the 5-Eyes, 9-Eyes, or 14-Eyes intelligence sharing agreements, preserving independent legal sovereignty.

Citation: International Surveillance Treaties [Ref 7].

8 DNS-Level NetShield Filtering

DNS BLOCKING

Correct Answer: True

TEACHING NOTE

NetShield intercepts DNS requests at the VPN gateway, resolving known malicious domains to 0.0.0.0 to prevent malware downloads.

Citation: Proton NetShield Docs [Ref 8].

9 Open Source Client Auditing

SECURITY TRANSPARENCY

Correct Answer: True

TEACHING NOTE

Proton is the first VPN provider to make all desktop and mobile apps fully open-source and publish complete third-party audit reports.

Citation: SEC Consult Security Report [Ref 9].

10 Stealth Header Obfuscation

OBFUSCATION TECH

Correct Answer: False

TEACHING NOTE

The Stealth protocol strips standard WireGuard handshake headers and scrambles packet size distributions to appear as ordinary HTTPS traffic.

Citation: Stealth Protocol Implementation [Ref 10].

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 SECURECR

B STEALTHP

C NETSHILD

D SWISSLWS

E KILLSWCH

F OPENSRC

G WIREGURD

H AES256GC

CHECKPOINT 3: KEY TERM KEY

1 SECURECR

2 STEALTHP

3 NETSHILD

4 SWISSLWS

5 KILLSWCH

6 OPENSRC

DISCUSSION NOTES FOR INSTRUCTORS

Protocol Performance:

Verify that students understand how WireGuard, OpenVPN, and proprietary protocols balance cryptographic overhead against throughput latency.

Privacy & Jurisdiction:

Emphasize the importance of independent third-party no-logs audits (Deloitte, Cure53, SEC Consult) and privacy-friendly legal havens.

Infrastructure Security:

Highlight kill-switch protection, RAM-only diskless server fleets, DNS leak prevention, and multi-hop routing configurations.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

E	S	Q	C	I	S	Y	W	G	M	J	I	O	X	B
N	Q	T	S	M	S	W	S	R	C	T	V	M	X	P
H	E	R	E	K	X	L	I	E	A	J	S	T	H	D
I	U	T	V	A	R	K	Z	S	C	R	A	G	U	P
W	W	W	S	J	L	X	O	W	S	U	E	I	Q	Y
W	I	I	Z	H	I	T	B	I	B	L	R	H	D	A
Q	S	R	A	B	I	B	H	Q	U	Y	W	E	D	V
L	A	P	E	A	F	L	O	P	Q	H	G	S	C	F
F	D	M	J	G	E	B	D	P	A	H	W	W	B	R
D	G	W	U	D	U	S	H	M	E	U	S	Q	U	P
S	N	J	K	E	V	R	2	X	K	N	I	V	X	X
L	G	I	H	X	G	H	D	5	S	G	S	T	A	O
F	I	F	N	L	R	T	C	F	6	H	T	R	H	W
A	K	I	L	L	S	W	C	H	W	G	S	E	C	H
E	O	R	J	N	Y	M	Z	K	E	Q	C	J	F	E

CROSSWORD SOLUTION

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

INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

- 1 Across:** **SECURECR** Hardened multi-hop bunker server routing. (8)
- 3 Across:** **STEALTHP** Obfuscation protocol bypassing restrictive firewalls. (8)
- 5 Across:** **NETSHIELD** DNS filter blocking trackers and malicious ads. (8)
- 7 Across:** **SWISSLWS** Strict non-EU legal privacy protections. (8)

DOWN CLUES

- 2 Down:** **KILLSWCH** Feature terminating network on tunnel disconnect. (8)
- 4 Down:** **OPENSRC** Audited software transparent to the public. (8)
- 6 Down:** **WIREGURD** Fast modern cryptographic tunneling protocol. (8)
- 8 Down:** **AES256GC** 256-bit Galois/Counter Mode encryption standard. (8)

Scrambled Words & Cipher Solution Key

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

WORD UNSCRAMBLE KEY

1. ECURECRS

SECURECR

5. ILLSWCHK

KILLSWCH

2. TEALTHPS

STEALTHP

6. PENSRCOE

OPENSRCOE

3. ETSHILDN

NETSHILD

7. IREGURDW

WIREGURD

4. WISSLWSS

SWISLWS

8. ES256GCA

AES256GC

SECRET CIPHER CHALLENGE KEY

"SECURE CORE HARDENED SERVERS PROTECT USER DATA"

VPN & Network Case Studies Solution Key

A CASE STUDY 1: BYPASSING RESTRICTIVE FIREWALLS

[Instructor Solution](#)

GRADING RUBRIC & SOLUTION GUIDELINES

Scenario Analysis: A user travels to a country where standard VPN traffic like OpenVPN and WireGuard is blocked by DPI.

Focus Question: Which Proton VPN protocol configuration allows the user to bypass state-level inspection?

Recommended Strategy & Solution: The user should activate the Stealth protocol, which obfuscates VPN packet headers as regular TLS/HTTPS web traffic, slipping past DPI filters.

B CASE STUDY 2: ADVANCED ADVERSARY PROTECTION

[Instructor Solution](#)

GRADING RUBRIC & SOLUTION GUIDELINES

Scenario Analysis: A financial auditor suspects their local ISP exit node might be compromised by advanced persistent threats.

Focus Question: How does Secure Core protect the auditor's identity against an exit node compromise?

Recommended Strategy & Solution: Secure Core routes traffic through hardened subterranean servers in Switzerland or Iceland first, ensuring the exit server cannot trace IP origin.

C CASE STUDY 3: MALWARE AND TRACKER PREVENTION

[Instructor Solution](#)

GRADING RUBRIC & SOLUTION GUIDELINES

Scenario Analysis: An enterprise employee frequently downloads research files from unfamiliar web forums.

Focus Question: Which integrated feature should be enabled to prevent malicious domains from resolving?

Recommended Strategy & Solution: Enabling NetShield at level 2 blocks malware, spyware, and advertising tracker domains at the DNS resolver level before packets reach the device.