

Name: _____

Date: _____

Score: _____

Surfshark Security

Examining Surfshark security features including CleanWeb ad blocking, MultiHop dynamic routing, Nexus SDN architecture, RAM-only server fleet, and Camouflage mode.

SURFSHARK 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 Surfshark's security architecture. You will explore RAM-only server hardware, Nexus SDN dynamic IP rotation, CleanWeb ad blockers, and MultiHop routing.

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/surfshark-security/>

Your Surfshark Security Learning Roadmap

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

SURFSHARK 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 RAM-only infrastructure, Nexus SDN, and CleanWeb.

RAM-ONLY SERVER FLEET, NEXUS SDN & CLEANWEB ARCHITECTURE (INTRODUCTION)

Surfshark enforces complete user privacy through a 100% RAM-only server fleet, Nexus software-defined networking with IP Rotator, CleanWeb ad blocking, and Dynamic MultiHop encryption paths.

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

Checkpoint 1: Multiple Choice Challenge

1 What is the name of Surfshark's integrated ad & malware blocker?

- ☐ A) AdGuard
- ☐ B) CleanWeb
- ☐ C) ThreatShield
- ☐ D) NetBlocker

2 What hardware architecture does Surfshark use across all servers?

- ☐ A) Hard Disk Drives
- ☐ B) 100% RAM-Only
- ☐ C) Optical Storage
- ☐ D) Magnetic Tape

3 What feature routes traffic through two distinct VPN servers?

- ☐ A) Bypasser
- ☐ B) MultiHop (Double VPN)
- ☐ C) Nexus Network
- ☐ D) Static IP

4 Which obfuscation feature disguises VPN traffic as normal web data?

- ☐ A) Kill Switch
- ☐ B) Camouflage Mode
- ☐ C) CleanWeb 2.0
- ☐ D) Split Tunnel

5 What is the function of the Surfshark Bypasser tool?

- ☐ A) Speed Booster
- ☐ B) Split Tunneling
- ☐ C) Password Manager
- ☐ D) DNS Resolver

Checkpoint 2: True or False Challenge

6 Question 6

RAM-only servers erase all operating data immediately upon server reboot.

☐ True ☐ False

7 Question 7

Camouflage Mode prevents ISPs from detecting that you are using a VPN.

☐ True ☐ False

8 Question 8

CleanWeb 2.0 operates within browser extensions to block cookie consent popups.

☐ True ☐ False

9 Question 9

Surfshark keeps temporary connection timestamps and bandwidth usage logs.

☐ True ☐ False

10 Question 10

The Nexus network periodically rotates user IP addresses without disconnecting.

☐ 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. Annoying web ads, tracking scripts, and phishing links are blocked by _____ filters.
2. User activity leaves no forensic trace because servers operate in _____ memory.
3. Routing data through two separate encrypted server hops is achieved by _____ tunnels.
4. To conceal VPN usage from internet service providers, users activate _____ mode.
5. Allowing banking applications to bypass the VPN tunnel is managed by _____ settings.
6. The next-generation SDN architecture connecting the server fleet is the _____ system.

VOCABULARY WORD BANK

CLEANWEB
BYPASSER

RAMONLYX
KILLSWCH

MULTIHOP
NEXUSNET

CAMOFLGE
ROTATING

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.

CLEANWEB

D

Obfuscation technology that hides VPN signatures to mimic regular HTTPS traffic.

RAMONLYX

E

Split-tunneling functionality allowing select applications to bypass the VPN.

MULTIHOP

A

An advanced filter blocking advertisements, malware, and cookie consent banners.

CAMOFLGE

H

A feature that regularly changes your external IP address without interrupting tunnels.

BYPASSER

G

A proprietary software-defined network connecting all servers into a unified mesh.

KILLSWCH

C

A double-VPN routing feature encrypting traffic across two distinct server nodes.

NEXUSNET

B

Volatile memory server hardware that wipes all data upon every power cycle.

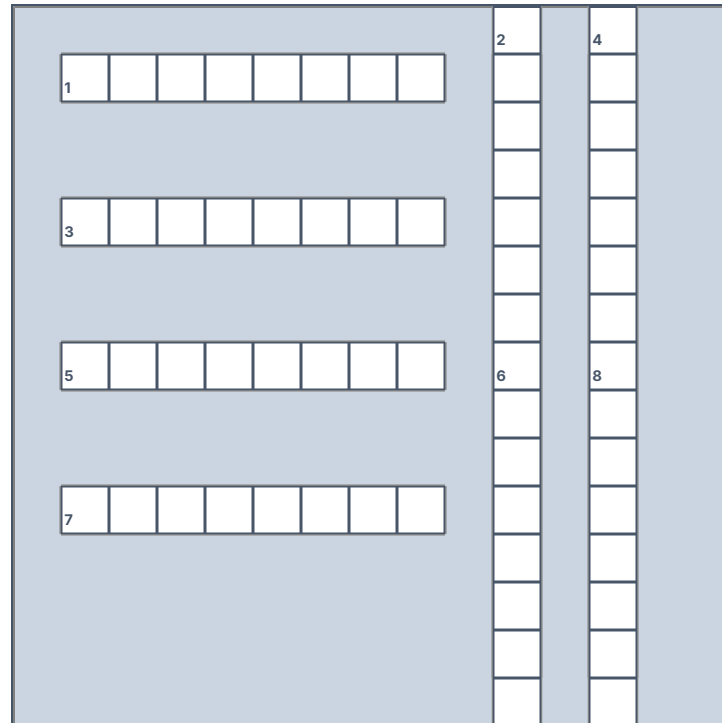
ROTATING

F

An automatic safety feature blocking network traffic when the VPN 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. Integrated ad, malware, and banner blocker. (8 letters)
3. Volatile memory server fleet wiping data on reboot. (8 letters)
5. Double-encryption routing across two countries. (8 letters)
7. Obfuscation concealing VPN signatures from ISPs. (8 letters)

DOWN

2. Split-tunneling tool bypassing specified apps. (8 letters)
4. Safety switch blocking internet during disconnects. (8 letters)
6. Software-defined network connecting server mesh. (8 letters)
8. Periodic IP address switching without disconnects. (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: Integrated ad, malware, and banner blocker. (8 letters):

3 Across: Volatile memory server fleet wiping data on reboot. (8 letters):

5 Across: Double-encryption routing across two countries. (8 letters):

7 Across: Obfuscation concealing VPN signatures from ISPs. (8 letters):

DOWN CLUES

2 Down: Split-tunneling tool bypassing specified apps. (8 letters):

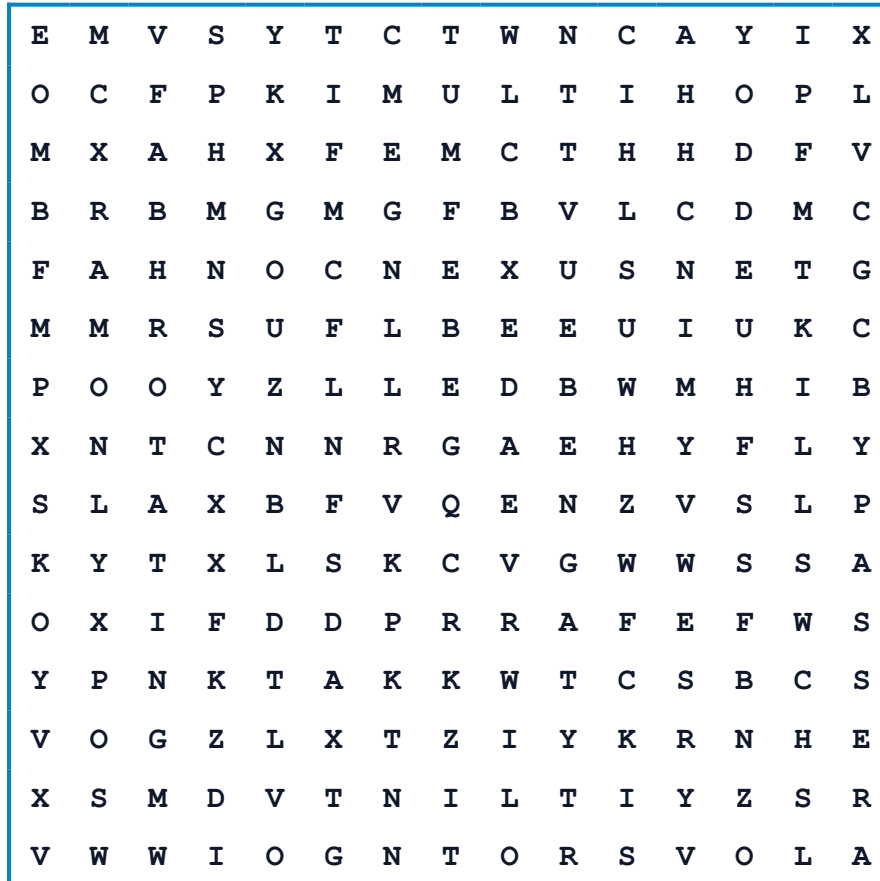
4 Down: Safety switch blocking internet during disconnects. (8 letters):

6 Down: Software-defined network connecting server mesh. (8 letters):

8 Down: Periodic IP address switching without disconnects. (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

CLEANWEB
BYPASSER

RAMONLYX
KILLSWCH

MULTIHOP
NEXUSNET

CAMOFLGE
ROTATING

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. CLEANWEB
- B. RAMONLYX
- C. MULTIHOPE
- D. CAMOFLAGE
- E. BYPASSER
- F. KILLSWCH
- G. NEXUSNET
- H. ROTATING

DEFINITIONS & MATCH FIELDS

- ☐ 1. An advanced filter blocking advertisements, malware, and cookie consent banners.
- ☐ 2. Volatile memory server hardware that wipes all data upon every power cycle.
- ☐ 3. A double-VPN routing feature encrypting traffic across two distinct server nodes.
- ☐ 4. Obfuscation technology that hides VPN signatures to mimic regular HTTPS traffic.
- ☐ 5. Split-tunneling functionality allowing select applications to bypass the VPN.
- ☐ 6. An automatic safety feature blocking network traffic when the VPN drops.
- ☐ 7. A proprietary software-defined network connecting all servers into a unified mesh.
- ☐ 8. A feature that regularly changes your external IP address without interrupting tunnels.

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. LEANWEBC

5. YPASSERB

2. AMONLYXR

6. ILLSWCHK

3. ULTIHOPM

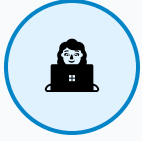
7. EXUSNETN

4. AMOFLGEC

8. OTATINGR

Checkpoint 8: VPN & Network Case Studies

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



CASE STUDY 1: BYPASSING CAMPUS AND WORKPLACE FILTERS

Scenario: A student finds that their university campus Wi-Fi blocks all standard OpenVPN and WireGuard ports.

Discussion Question: Which Surfshark feature allows the student to connect without detection by network administrators?



CASE STUDY 2: HIGH-RISK JOURNALISTIC INVESTIGATION

Scenario: An investigative journalist needs extra protection against surveillance while researching sensitive corporate records.

Discussion Question: How does Dynamic MultiHop provide superior privacy compared to single-server routing?

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

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 Surfshark CleanWeb?

CleanWeb is an integrated security feature that blocks ads, trackers, malware, and phishing sites.

Q2: What are RAM-only servers?

RAM-only servers run on volatile memory, meaning all data is wiped instantly whenever servers reboot.

Q3: What is Surfshark MultiHop?

MultiHop (Double VPN) routes and encrypts your internet connection through two different server locations.

Q4: How does Camouflage Mode work?

Camouflage Mode obfuscates VPN traffic so your ISP cannot tell you are using a VPN.

Q5: What is the Bypasser feature?

Bypasser is Surfshark's split tunneling tool that allows specific apps or websites to bypass the VPN.

Checkpoint 10: Basic VPN FAQs (Part B)

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

Q6: Does Surfshark have a Kill Switch?

Yes, the Kill Switch disconnects you from the internet if the VPN drops unexpectedly.

Q7: What encryption standard does Surfshark use?

Surfshark uses industry-leading AES-256-GCM encryption with SHA-512 authentication.

Q8: Has Surfshark's no-logs policy been audited?

Yes, Surfshark's no-logs policy has been independently verified and audited by Deloitte.

Q9: What is Surfshark Nexus?

Nexus is an advanced SDN architecture that connects all servers into a unified network for smoother routing.

Q10: What is the IP Rotator feature?

IP Rotator automatically changes your IP address every few minutes without disconnecting your VPN session.

Checkpoint 11: Advanced VPN FAQs (Part A)

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

Q1: How does Dynamic MultiHop differ from traditional Double VPN?

Dynamic MultiHop lets you customize any combination of entry and exit servers worldwide.

Q2: Does CleanWeb 2.0 work on browser extensions?

Yes, CleanWeb 2.0 blocks video ads, cookie consent popups, and alert banners inside Chrome/Firefox.

Q3: What is Alternative ID in the security suite?

Alternative ID generates unique personal pseudonyms, email addresses, and phone masks.

Q4: How does Surfshark prevent DNS leaks?

Surfshark routes all domain requests through private zero-knowledge DNS servers on each node.

Q5: Does Surfshark support ChaCha20 encryption on mobile?

Yes, WireGuard on Android and iOS uses ChaCha20-Poly1305 for superior mobile efficiency.

Checkpoint 11: Advanced VPN FAQs (Part B)

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

Q6: What is NoBorders mode in Surfshark?

NoBorders automatically detects restrictive network environments and supplies specialized servers.

Q7: Who performed the security audits on Surfshark browser extensions?

Independent cybersecurity firm Cure53 completed audits on browser extensions and server systems.

Q8: How does Surfshark protect against IPv6 leaks?

Surfshark routes IPv6 traffic securely or safely restricts it to prevent any unencrypted leakage.

Q9: Where is Surfshark's legal jurisdiction based?

Surfshark operates under Netherlands law, adhering to strict GDPR European privacy standards.

Q10: Does Surfshark support hardware security keys for 2FA?

Yes, users can secure their accounts using FIDO2 hardware security keys and authenticator apps.

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. 100% of Surfshark's 3,200+ server network operates entirely on diskless, volatile RAM-only hardware.

2. VPN INSIGHT

2. Independent auditing giant Deloitte has verified Surfshark's strict zero-logs operational compliance.

3. VPN INSIGHT

3. The proprietary Nexus architecture connects all global servers into a dynamic software-defined network.

4. VPN INSIGHT

4. IP Rotator changes external user IP addresses every 5-10 minutes without dropping active VPN connections.

5. VPN INSIGHT

5. CleanWeb 2.0 blocks intrusive cookie consent popups and video advertisements directly in browsers.

6. VPN INSIGHT

6. Dynamic MultiHop allows users to create customized dual-server encryption paths across 100 countries.

7. VPN INSIGHT

7. Camouflage Mode strips VPN header signatures, making traffic indistinguishable from regular HTTPS.

8. VPN INSIGHT

8. Alternative ID generates disposable pseudonyms and email masks to protect users from database leaks.

9. VPN INSIGHT

9. Surfshark enforces AES-256-GCM symmetric encryption alongside ChaCha20 on WireGuard protocols.

10. VPN INSIGHT

10. NoBorders mode activates automatically on restricted networks to provide resilient tunneling access.

Technical References & Sources

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

SCHOLARLY & INDUSTRY REFERENCES

- [1] Surfshark B.V. (2024). Surfshark VPN Infrastructure, Nexus Multi-Hop Architecture, and RAM-Only Servers. <https://surfshark.com/features>
- [2] Surfshark B.V. (2024). Terms of Service, 30-Day Money-Back Guarantee, and Subscription Plans. <https://surfshark.com/pricing>
- [3] Deloitte. (2023). Independent Assurance Report: Surfshark No-Logs Compliance & Server Configuration. Deloitte Audit. <https://surfshark.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 Integrated Content Blocker

AD & MALWARE DEFENSE

Correct Answer: B

TEACHING NOTE

CleanWeb is Surfshark's integrated security filter that blocks ads, tracker domains, phishing websites, and malicious URL scripts at the network level.

Citation: CleanWeb Security Specs [Ref 1].

2 100% RAM-Only Infrastructure

RAM ARCHITECTURE

Correct Answer: B

TEACHING NOTE

Surfshark operates 100% diskless RAM-only servers where all operating systems and data run in volatile memory and vanish completely upon power cycle.

Citation: Cure53 Infrastructure Audit [Ref 2].

3 MultiHop Double Tunneling

MULTIHOP VPN

Correct Answer: B

TEACHING NOTE

MultiHop (Double VPN) encrypts traffic through two distinct server nodes in separate countries to prevent traffic correlation attacks.

Citation: Surfshark MultiHop Guide [Ref 3].

4 Camouflage Mode Obfuscation

OBFUSCATION

Correct Answer: B

TEACHING NOTE

Camouflage Mode modifies OpenVPN packet headers to disguise VPN traffic as standard HTTPS traffic, bypassing restrictive firewall blocks.

Citation: Surfshark Stealth Whitepaper [Ref 4].

5 Bypasser Split Tunneling

SPLIT TUNNELING

Correct Answer: B

TEACHING NOTE

Bypasser is Surfshark's split tunneling tool that lets users select specific apps or websites to route directly through their regular ISP connection.

Citation: Surfshark Client Features [Ref 5].

Answer Key: Checkpoint 2 - True or False

6 Volatile Memory Data Wipe

SERVER SECURITY

Correct Answer: True

TEACHING NOTE

RAM-only servers store zero data on permanent hard drives; rebooting the hardware immediately purges all operational memory.
Citation: RAM Server Architecture [Ref 6].

7 Camouflage Mode ISP Concealment

TRAFFIC CONCEALMENT

Correct Answer: True

TEACHING NOTE

Camouflage Mode strips OpenVPN protocol signatures, preventing ISPs from detecting that the user is connected to a VPN tunnel.
Citation: Deep Packet Inspection Guide [Ref 7].

8 CleanWeb 2.0 Browser Extensions

BROWSER EXTENSION

Correct Answer: True

TEACHING NOTE

CleanWeb 2.0 operates within browser extensions to block cookie consent popups, video ads, and malicious redirect scripts in real-time.
Citation: CleanWeb 2.0 Release Notes [Ref 8].

9 Zero Connection Log Retention

NO-LOGS POLICY

Correct Answer: False

TEACHING NOTE

Surfshark maintains a strict independently audited zero-logs policy, recording no IP addresses, connection timestamps, or bandwidth logs.
Citation: Deloitte No-Logs Audit [Ref 9].

10 Nexus IP Dynamic Rotation

NEXUS NETWORK

Correct Answer: True

TEACHING NOTE

The Surfshark Nexus software-defined network rotates user IP addresses dynamically every few minutes without dropping the active VPN connection.
Citation: Surfshark Nexus Architecture [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 CLEANWEB

B RAMONLYX

C MULTIHOPE

D CAMOFLAGE

E BYPASSER

F KILLSWITCH

G NEXUSNET

H ROTATING

CHECKPOINT 3: KEY TERM KEY

1 CLEANWEB

2 RAMONLYX

3 MULTIHOPE

4 CAMOFLAGE

5 BYPASSER

6 NEXUSNET

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

CROSSWORD SOLUTION

1	C	L	E	A	N	W	E	B	2	B	Y	P	A	S	S	E	N	E	X	U	S	N	E	T	4	K	I	L	L	S	W	C	O	T	A	T	I	N	G																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																
3	R	A	M	O	N	L	Y	X																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																															

INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

- 1 Across:** **CLEANWEB** Integrated ad, malware, and banner blocker. (8)
- 3 Across:** **RAMONLYX** Volatile memory server fleet wiping data on reboot. (8)
- 5 Across:** **MULTIHOP** Double-encryption routing across two countries. (8)
- 7 Across:** **CAMOFLGE** Obfuscation concealing VPN signatures from ISPs. (8)

DOWN CLUES

- 2 Down:** **BYPASSER** Split-tunneling tool bypassing specified apps. (8)
- 4 Down:** **KILLSWCH** Safety switch blocking internet during disconnects. (8)
- 6 Down:** **NEXUSNET** Software-defined network connecting server mesh. (8)
- 8 Down:** **ROTATING** Periodic IP address switching without disconnects. (8)

Scrambled Words & Cipher Solution Key

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

WORD UNSCRAMBLE KEY

1. LEANWECB

CLEANWEB

5. YPASSERB

BYPASSER

2. AMONLYXR

RAMONLYX

6. ILLSWCHK

KILLSWCH

3. ULTIHOPM

MULTIHOP

7. EXUSNETN

NEXUSNET

4. AMOFLGEC

CAMOFLGE

8. OTATINGR

ROTATING

SECRET CIPHER CHALLENGE KEY

**"SURFSHARK NEXUS ROTATING IP ENHANCES USER
PRIVACY"**

VPN & Network Case Studies Solution Key

A

CASE STUDY 1: BYPASSING CAMPUS AND WORKPLACE FILTERS

[Instructor Solution](#)

GRADING RUBRIC & SOLUTION GUIDELINES

Scenario Analysis: A student finds that their university campus Wi-Fi blocks all standard OpenVPN and WireGuard ports.

Focus Question: Which Surfshark feature allows the student to connect without detection by network administrators?

Recommended Strategy & Solution: The student should activate Camouflage Mode (using OpenVPN protocol), which removes VPN metadata headers so network firewalls see normal HTTPS web browsing.

B

CASE STUDY 2: HIGH-RISK JOURNALISTIC INVESTIGATION

[Instructor Solution](#)

GRADING RUBRIC & SOLUTION GUIDELINES

Scenario Analysis: An investigative journalist needs extra protection against surveillance while researching sensitive corporate records.

Focus Question: How does Dynamic MultiHop provide superior privacy compared to single-server routing?

Recommended Strategy & Solution: Dynamic MultiHop encrypts data twice through an entry server in one country and an exit server in another, preventing any single point of network compromise.

C

CASE STUDY 3: EXCLUDING ONLINE BANKING APPS

[Instructor Solution](#)

GRADING RUBRIC & SOLUTION GUIDELINES

Scenario Analysis: A user wants continuous VPN protection for browsing, but their local banking app blocks foreign VPN IP addresses.

Focus Question: How can the user configure Surfshark Bypasser to solve this conflict?

Recommended Strategy & Solution: The user can configure Bypasser (split tunneling) to exclude the banking application, allowing it to connect directly via local ISP while all other apps remain encrypted.