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

ON
LEAK PROTECTION
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.**
- [ ] **Bonus: Think Fast challenge.**

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. Finish with the Bonus Activity: Think Fast.

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

Surfshark protects user privacy with an all-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

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

○ True ○ False

7 Question 7

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

○ True ○ False

8 Question 8

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

○ True ○ False

9 Question 9

9. Surfshark keeps temporary connection timestamps and bandwidth usage logs.

○ True ○ False

10 Question 10

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

BYPASSER CAMOUFLAGE CLEANWEB KILL SWITCH MULTIHOP NEXUS RAM-ONLY ROTATING IP

Write your answers here:

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

Checkpoint 4: VPN & Network Concept Match

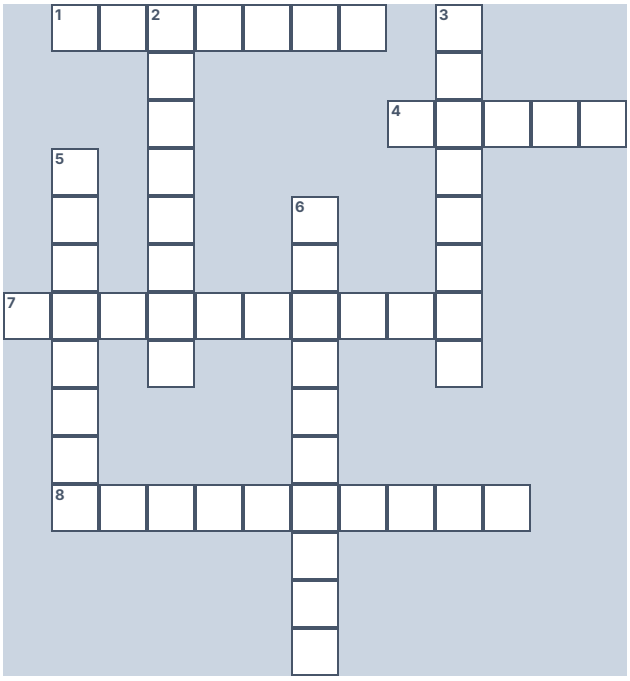
DEFINITION MATCHING

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.

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

Checkpoint 5: Crossword Puzzle

Solve the crossword puzzle by typing letters into the active white boxes. The numbers correspond to the clues below.



ACROSS CLUES

1. Volatile memory server hardware that wipes all data upon every power cycle (7)

4. A proprietary software-defined network connecting all servers into a unified mesh (5)

7. Obfuscation technology that hides VPN signatures to mimic regular HTTPS traffic (10)

8. A feature that regularly changes your external IP address without interrupting tunnels (10)

DOWN CLUES

2. A double-VPN routing feature encrypting traffic across two distinct server nodes (8)

3. An advanced filter blocking advertisements, malware, and cookie consent banners (8)

5. Split-tunneling functionality allowing select applications to bypass the VPN (8)

6. An automatic safety feature blocking network traffic when the VPN drops (10)

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: Volatile memory server hardware that wipes all data upon every power cycle (7 letters):

4 Across: A proprietary software-defined network connecting all servers into a unified mesh (5 letters):

7 Across: Obfuscation technology that hides VPN signatures to mimic regular HTTPS traffic (10 letters):

8 Across: A feature that regularly changes your external IP address without interrupting tunnels (10 letters):

DOWN CLUES

2 Down: A double-VPN routing feature encrypting traffic across two distinct server nodes (8 letters):

3 Down: An advanced filter blocking advertisements, malware, and cookie consent banners (8 letters):

5 Down: Split-tunneling functionality allowing select applications to bypass the VPN (8 letters):

6 Down: An automatic safety feature blocking network traffic when the VPN drops (10 letters):

Checkpoint 6: Hidden Word Search

Find the 8 key vocabulary terms hidden in the grid below. Words can be horizontal, vertical, or diagonal.

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

VOCABULARY WORD LIST

CLEANWEB RAMONLY MULTIHOP NEXUS CAMOUFLAGE ROTATINGIP BYPASSER KILLSWITCH

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. RAMONLY**
- **C. MULTIHOP**
- **D. CAMOUFLAGE**
- **E. BYPASSER**
- **F. KILLSWITCH**
- **G. NEXUS**
- **H. ROTATINGIP**

DEFINITIONS & MATCH FIELDS

_____ 1. Obfuscation technology that hides VPN signatures to mimic regular HTTPS traffic.

_____ 2. An automatic safety feature blocking network traffic when the VPN drops.

_____ 3. An advanced filter blocking advertisements, malware, and cookie consent banners.

_____ 4. Split-tunneling functionality allowing select applications to bypass the VPN.

_____ 5. Volatile memory server hardware that wipes all data upon every power cycle.

_____ 6. A feature that regularly changes your external IP address without interrupting tunnels.

_____ 7. A double-VPN routing feature encrypting traffic across two distinct server nodes.

_____ 8. A proprietary software-defined network connecting all servers into a unified mesh.

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. EANCWLBE
2. TMPUOHIL
3. AYBSSREP
4. XSUNE
5. NYOMRLA
6. GUOLACAFEM
7. ILKIWTCHSL
8. IAIPRTONGT

Bonus Activity: Think Fast

3 ITEMS FROM EACH CATEGORY. FIRST PERSON TO COMPLETE THE LIST WINS.

1	Security features in Surfshark			
2	Signs your VPN connection is slow			
3	VPN protocols you know			
4	Things encryption protects			
5	Threats on public Wi-Fi			
6	Countries known for strong privacy laws			
7	Ways to make a strong password			
8	Devices you would install Surfshark on			
9	Questions for Surfshark customer support			
10	Settings you turn on for extra security			
11	Things Surfshark can hide from your network			
12	Types of VPN leaks			
13	Data a VPN should never store			
14	Words that describe a good VPN app			
15	Things an audit can check			

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?

Checkpoint 9: 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 21 18 6 19 8 1 18 11 14 5 24 21 19

18 15 20 1 20 9 14 7 9 16 5 14 8 1 14 3 5 19

21 19 5 18 16 18 9 22 1 3 25

Decoded 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 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 data held in memory is wiped 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. [9]

Q7: What encryption standard does Surfshark use?

Surfshark uses AES-256-GCM and ChaCha20, plus AEGIS-256X2 on its new Dausos protocol.

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

Yes, Deloitte verified Surfshark's no-logs policy in 2023 and again in 2025.

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 10: Advanced VPN FAQs (Part C)

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. [11]

Q4: How does Surfshark prevent DNS leaks?

Surfshark routes all domain requests through its own private 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 10: Advanced VPN FAQs (Part D)

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. [10]

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. [7]

Q10: Does Surfshark support two-factor authentication (2FA)?

Yes, and Surfshark One adds a 2FA lock so only you can change feature settings.

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. Surfshark says its entire 4,500+ server network runs on diskless, volatile RAM-only hardware. [8]

2. VPN INSIGHT

2. Big Four firm Deloitte verified Surfshark's no-logs policy in 2023 and again in November 2025. [2]

3. VPN INSIGHT

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

4. VPN INSIGHT

4. Rotating IP changes your IP address about every five minutes without dropping the VPN connection. [6]

5. VPN INSIGHT

5. CleanWeb 2.0 blocks intrusive cookie consent popups and video advertisements directly in browsers. [4]

6. VPN INSIGHT

6. Dynamic MultiHop allows users to create customized dual-server encryption paths across 100 countries. [5]

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. [3]

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. (n.d.). Welcome to Surfshark's trust center!
https://surfshark.com/trust-center

[2] Surfshark. (2025). Our no-logs policy was verified again.
https://surfshark.com/blog/deloitte-nologs-policy-verified-again

[3] Surfshark. (n.d.). Surfshark VPN protocols: Dausos, WireGuard, OpenVPN, IKEv2.
https://surfshark.com/features/surfshark-vpn-protocols

[4] Surfshark. (n.d.). Clean Web: VPN ad blocker for safe and ad-free browsing.
https://surfshark.com/features/cleanweb

[5] Surfshark. (n.d.). What is double VPN and when to use it.
https://surfshark.com/features/multihop

[6] Surfshark. (n.d.). Rotating IP: rotate your IP for extra privacy.
https://surfshark.com/features/ip-rotator

[7] Surfshark. (n.d.). Surfshark Privacy Policy.
https://surfshark.com/privacy

[8] Surfshark. (n.d.). Surfshark VPN servers: location list.
https://surfshark.com/servers

[9] Surfshark. (n.d.). VPN kill switch: protection that never slips.
https://surfshark.com/features/kill-switch

[10] Surfshark. (2023). Surfshark server infrastructure undergoes an independent audit.
https://surfshark.com/blog/surfshark-server-infrastructure-undergoes-independent-audit

[11] Surfshark. (n.d.). Alternative ID & Alternative Number.
https://surfshark.com/alternative-id

[12] Surfshark. (n.d.). What are obfuscated servers & why you need them.
https://surfshark.com/features/obfuscated-servers

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.

2 **100% RAM-Only Infrastructure** RAM ARCHITECTURE — **Correct Answer: B**

TEACHING NOTE

Surfshark runs RAM-only servers, so data held in server memory is wiped when a server is powered off or rebooted.

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.

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.

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.

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.

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.

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.

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.

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.

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

C 1. CLEANWEB	D 2. RAM-ONLY	G 3. MULTIHOP	F 4. CAMOUFLAGE
B 5. BYPASSER	A 6. KILL SWITCH	H 7. NEXUS	E 8. ROTATING IP

CHECKPOINT 3: KEY TERM KEY

1 CLEANWEB	2 RAM-ONLY	3 MULTIHOP	4 CAMOUFLAGE
5 BYPASSER	6 NEXUS		

CHECKPOINT 6 ALTERNATIVE: VOCABULARY MATCH KEY

1 D – CAMOUFLAGE	2 F – KILLSWITCH	3 A – CLEANWEB	4 E – BYPASSER
5 B – RAMONLY	6 H – ROTATINGIP	7 C – MULTIHOP	8 G – NEXUS

DISCUSSION NOTES FOR INSTRUCTORS

Key Terms:
Check that students can explain CLEANWEB, RAM-ONLY and MULTIHOP in their own words and give an example of each.

Case Studies:
Ask students to support their recommendations with facts from the worksheet rather than assumptions.

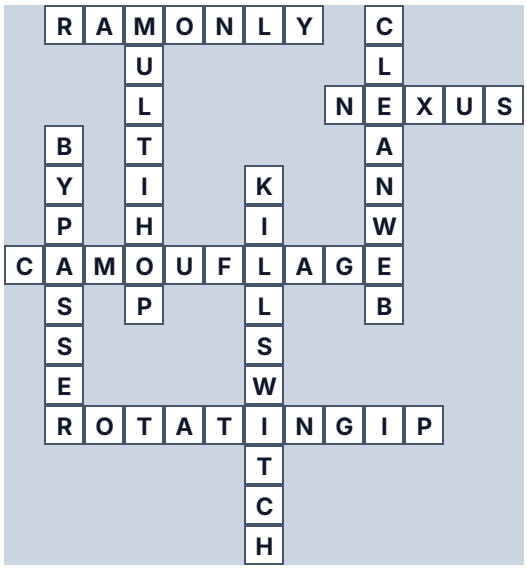
Source Evaluation:
Have students verify at least one claim against the worksheet references, and discuss why figures, prices and rules can change over time.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

CROSSWORD SOLUTION



INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

1 Across: RAMONLY Volatile memory server hardware that wipes all data upon every power cycle (7 letters)

4 Across: NEXUS A proprietary software-defined network connecting all servers into a unified mesh (5 letters)

7 Across: CAMOUFLAGE Obfuscation technology that hides VPN signatures to mimic regular HTTPS traffic (10 letters)

8 Across: ROTATINGIP A feature that regularly changes your external IP address without interrupting tunnels (10 letters)

DOWN CLUES

2 Down: MULTIHOP A double-VPN routing feature encrypting traffic across two distinct server nodes (8 letters)

3 Down: CLEANWEB An advanced filter blocking advertisements, malware, and cookie consent banners (8 letters)

5 Down: BYPASSER Split-tunneling functionality allowing select applications to bypass the VPN (8 letters)

6 Down: KILLSWITCH An automatic safety feature blocking network traffic when the VPN drops (10 letters)

Scrambled Words & Cipher Solution Key

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

WORD UNSCRAMBLE KEY

1. EANCWLBE	CLEANWEB	5. NYOMRLA	RAMONLY
2. TMPUOHIL	MULTIHOP	6. GUOLACAFEM	CAMOUFLAGE
3. AYBSSREP	BYPASSER	7. ILKIWTCHSL	KILLSWITCH
4. XSUNE	NEXUS	8. IAIPRTONGT	ROTATINGIP

SECRET CIPHER CHALLENGE KEY

"SURFSHARK NEXUS ROTATING IP ENHANCES USER PRIVACY"

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: Activate Camouflage Mode (OpenVPN), which hides VPN metadata so firewalls see normal HTTPS 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 routes traffic through entry and exit servers in two countries, so no single server can expose the user.