Name: _____ Date: _____ Score: _____

Avast SecureLine VPN

Evaluating Avast SecureLine VPN logging policies, proprietary protocols, and platform performance.

AVAST SECURELINE 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 Avast SecureLine VPN. You will explore Czech jurisdiction, Mimic proprietary protocols, AES-256 standard encryption, logging policies, and client features.

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/avast-secureline-vpn/

Your Avast SecureLine VPN Learning Roadmap

- Analyze Avast's logging policy and telemetry data aggregation.
- Evaluate the performance of Mimic and OpenVPN protocols.
- Map the global server network size and IP address diversity.
- Compare connection latency and speed loss ratios.
- Install and configure SecureLine clients on Windows and macOS.

AVAST SECURELINE VPN 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 Czech legal jurisdiction and Mimic protocol.

CZECH LEGAL JURISDICTION & MIMIC PROTOCOL (INTRODUCTION)

Avast SecureLine VPN utilizes its proprietary Mimic protocol and standard AES-256 encryption to protect user connections. Operating under Czech jurisdiction, it complies with EU data rules while providing optimized streaming and sharing servers.

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

Checkpoint 1: Multiple Choice Challenge

1 **What is the name of Avast SecureLine's proprietary connection protocol?**

- A) Mimic
- B) NordLynx
- C) Lightway
- D) Stealth

2 **Where is Avast officially headquartered?**

- A) Czech Republic
- B) United States
- C) Switzerland
- D) Panama

3 **What encryption standard does Avast SecureLine VPN use by default?**

- A) AES-256
- B) ChaCha20
- C) Blowfish
- D) DES

4 **How many simultaneous device links does the multi-device plan allow?**

- A) Ten links
- B) Five links
- C) Two links
- D) Unlimited links

5 **What session metric does Avast admit to logging in its policy?**

- A) Connection timestamps
- B) Visited URLs
- C) Transmitted files
- D) Search queries

Checkpoint 2: True or False Challenge

6 Question 6

Avast SecureLine VPN uses the Mimic protocol to bypass censorship blocking.

◯ True ◯ False

7 Question 7

Avast VPN maintains a fully audited, zero-logs server architecture.

◯ True ◯ False

8 Question 8

SecureLine VPN offers dedicated servers optimized for P2P file sharing.

◯ True ◯ False

9 Question 9

The Czech Republic jurisdiction is completely free from EU data retention laws.

◯ True ◯ False

10 Question 10

Avast VPN includes a system-wide Kill Switch on both Windows and macOS.

◯ 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. Avast's proprietary protocol designed to bypass local firewalls is called _____.

2. The provider is subject to EU data laws due to its _____ jurisdiction.

3. Traffic payload data is secured using the standard _____ encryption algorithm.

4. The multi-device subscription plan allows a maximum of _____ connected at once.

5. Avast's logging policy admits to recording connection _____ for billing.

6. To prevent unencrypted traffic leaks, you must enable the client _____.

VOCABULARY WORD BANK

MIMIC	CZECH	AES256	TENDEVICES
TIMESTAMPS	KILLSWITCH	PEERTOPEER	OVERHEAD

Write your answers here:

1. **2.**

3. **4.**

5. **6.**

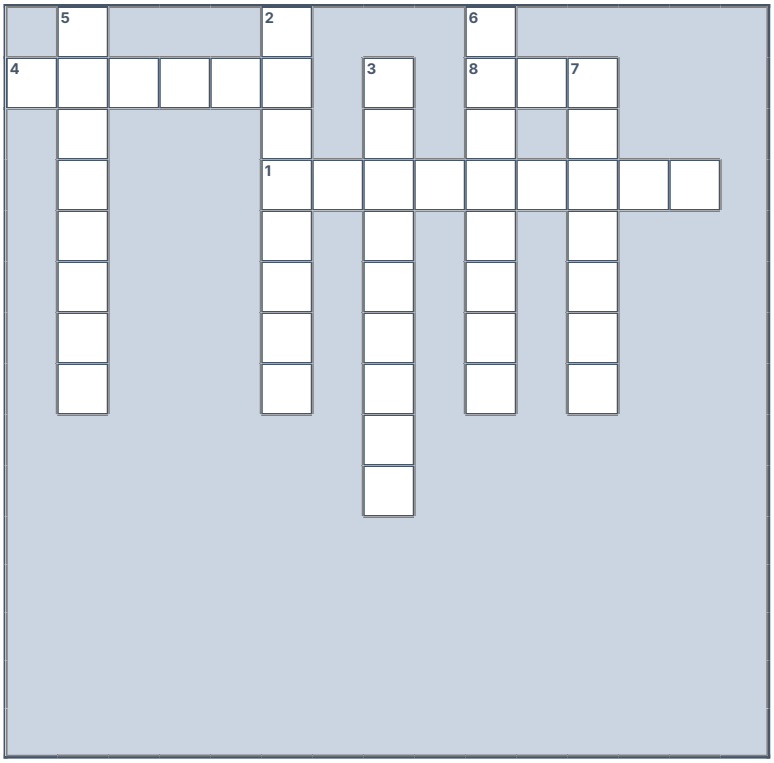
Checkpoint 4: Domain Concept Match

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.

( )	MIMIC	E	Logged session connection metrics.
( )	CZECH	F	Local firewall rule blocking leaks.
( )	AES256	G	Dedicated server categories for sharing.
( )	TENDEVICES	C	Industrial-strength encryption standard.
( )	TIMESTAMPS	A	Proprietary Avast VPN protocol.
( )	KILLSWITCH	B	Central European legal jurisdiction.
( )	PEERTOPEER	H	CPU processing cost of encryption.
( )	OVERHEAD	D	Multi-device subscription link limit.

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: Proprietary Avast VPN protocol. (5 letters):

3 Across: Industrial-strength encryption standard. (6 letters):

5 Across: Logged session connection metrics. (10 letters):

7 Across: Dedicated server categories for sharing. (10 letters):

DOWN CLUES

2 Down: Central European legal jurisdiction. (5 letters):

4 Down: Multi-device subscription link limit. (10 letters):

6 Down: Local firewall rule blocking leaks. (10 letters):

8 Down: CPU processing cost of encryption. (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.

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

VOCABULARY WORD LIST

MIMIC	CZECH	AES256	TENDEVICES
TIMESTAMPS	KILLSWITCH	PEERTOPEER	OVERHEAD

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. MIMIC
B. CZECH
C. AES256
D. TENDEVICES
E. TIMESTAMPS
F. KILLSWITCH
G. PEERTOPEER
H. OVERHEAD

DEFINITIONS & MATCH FIELDS

_____ 1. Proprietary Avast VPN protocol.

_____ 2. Central European legal jurisdiction.

_____ 3. Industrial-strength encryption standard.

_____ 4. Multi-device subscription link limit.

_____ 5. Logged session connection metrics.

_____ 6. Local firewall rule blocking leaks.

_____ 7. Dedicated server categories for sharing.

_____ 8. CPU processing cost of encryption.

Checkpoint 7: Scrambled Word Challenge

Unscramble the letters below to reveal key domain brokerage concepts and terms. Write your answers in the input boxes provided.

1. CMIIM

2. HCCEZ

3. S652AE

4. CEDISVETEN

5. MSTEPMASIT

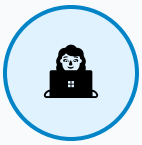
6. TLIWCHISKL

7. REREOPTEPE

8. RDVAEOHE

Checkpoint 8: Domain Brokerage Case Studies

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



CASE STUDY 1: LOGGING COMPLIANCE

Scenario: A user reviews Avast's logging policy and notices that while browsing data is not stored, Avast records connection durations and raw bandwidth usage for capacity planning.

Discussion Question: What session metric does Avast log temporarily to monitor infrastructure loads?

CASE STUDY 2: FIREWALL BYPASS

Scenario: An engineer tries to bypass a network firewall that blocks OpenVPN traffic by scanning packet headers. They need a protocol that disguises VPN packets as standard HTTPS data.

Discussion Question: Which Avast SecureLine protocol option is designed to evade this deep packet filtering?

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

13	9	13	9	3		16	18	15	20	15	3	15	12
5	22	1	4	5	19		6	9	18	5	23	1	12	12
4	5	20	5	3	20	9	15	14		18	21	12	5	19

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 is Avast SecureLine VPN?

A subscription-based VPN service developed by Avast, focused on security integration inside the Avast ecosystem.

Q2: What is the Mimic protocol?

Avast's proprietary connection protocol designed to mask VPN signatures and bypass deep packet inspection rules.

Q3: Where is Avast VPN located?

It is based in Prague, Czech Republic, placing it under EU legal and data regulations.

Q4: Does Avast SecureLine keep logs?

Their policy admits to logging connection timestamps, active device count, and overall bandwidth usage, though not user browsing history.

Q5: What is the encryption standard used by Avast?

It utilizes AES-256 encryption in combination with OpenVPN and Mimic protocols.

Checkpoint 10: Basic VPN FAQs (Part B)

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

Q6: Can I connect multiple devices to Avast VPN?

Yes, their multi-device plan allows up to ten simultaneous device connections under a single account.

Q7: Does Avast VPN support P2P file sharing?

Yes, they provide dedicated servers labeled for P2P and torrenting traffic in select locations.

Q8: What is the role of the Avast Kill Switch?

It blocks all internet access if the VPN connection drops, preventing unsecured data leakage.

Q9: Does Avast secure public Wi-Fi connections?

Yes, it can be configured to automatically connect whenever an unsecured Wi-Fi network is detected.

Q10: What is the refund window for Avast SecureLine?

Avast provides a standard 30-day money-back guarantee for its VPN subscription tiers.

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 Mimic protocol bypass deep packet inspection?

By restructuring and mapping packet headers to mimic standard HTTPS transactions, evading automated firewall filtering.

Q2: What are the legal implications of the Czech Republic jurisdiction?

As an EU member state, it complies with GDPR but is also subject to European data retention requests and intelligence sharing.

Q3: Why does Avast log connection timestamps?

Avast uses connection metrics to enforce active device limits and monitor server capacity thresholds in real time.

Q4: How does Avast SecureLine protect against DNS leaks?

The client routes all DNS lookups through private Avast DNS servers, overriding local ISP network adapter settings.

Q5: What is the speed overhead of the Mimic protocol?

Due to additional packet wrapping and header modifications, Mimic can introduce slightly higher CPU latency than WireGuard.

Checkpoint 11: Advanced VPN FAQs (Part B)

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

Q6: Can I set up Avast VPN on my router?

Avast does not provide dedicated router applets, but manual configurations are supported on OpenVPN-capable routers.

Q7: How does Avast's system-level Kill Switch differ from competitor apps?

It binds directly to the network interface card driver, disabling routing rather than killing individual applications.

Q8: Does Avast VPN support split tunneling?

Yes, split tunneling is supported on Android and Windows clients, allowing select apps to bypass encryption.

Q9: How does Avast handle WebRTC leak protection?

The client configures local routing tables to block browser WebRTC queries from exposing the true public IP.

Q10: Why is the Czech Republic outside the primary Five Eyes alliance?

It is not a formal member, but cooperates with Western agencies under EU-wide mutual legal assistance treaties.

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

Avast's proprietary Mimic protocol is engineered to bypass strict network blockages by mimicking HTTPS headers.

2. VPN INSIGHT

Avast VPN is incorporated in the Czech Republic, subjecting it to European data privacy regulations.

3. VPN INSIGHT

The multi-device plan from Avast allows up to ten simultaneous device connections under one account.

4. VPN INSIGHT

Avast logs connection durations and bandwidth data but does not record visited web domains.

5. VPN INSIGHT

Dedicated P2P servers are labeled in the client to ensure high throughput for file sharing.

6. VPN INSIGHT

Avast SecureLine uses AES-256 encryption, a standard approved for securing confidential government data.

7. VPN INSIGHT

The client includes auto-secure rules to enable protection whenever a public Wi-Fi network is detected.

8. VPN INSIGHT

DNS leak protection forces all name resolution queries through secure, private Avast DNS servers.

9. VPN INSIGHT

A 30-day money-back guarantee is provided for all new SecureLine subscription plans.

10. VPN INSIGHT

Czech Republic cooperation with EU agencies is governed by Mutual Legal Assistance Treaties.

Technical References & Sources

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

SCHOLARLY & INDUSTRY REFERENCES

[1] Avast SecureLine VPN Privacy Policy and Logging. Retrieved from https://www.avast.com/privacy-policy

[2] Mimic Connection Protocol Specification and Technology. Retrieved from https://www.avast.com/technology

[3] Czech Republic Act on Electronic Communications. Retrieved from https://www.mpo.cz/en/

[4] Advanced Encryption Standard (AES) Security and Overview. Retrieved from https://www.nist.gov/

[5] Avast Multi-Device Subscription Plan Guidelines. Retrieved from https://www.avast.com/pricing

[6] Peer-to-Peer (P2P) File Sharing Server Design. Retrieved from https://www.vpn.com/p2p/

[7] IETF RFC 5246: The Transport Layer Security (TLS) Protocol. Retrieved from https://datatracker.ietf.org/doc/rfc5246/

[8] Windows VPN Adapters and Routing Metrics. Retrieved from https://www.microsoft.com/

[9] CPU Overhead and Cryptographic Latency Studies. Retrieved from https://www.vpn.com/reviews/

[10] Avast SecureLine Client Troubleshooting and Manuals. Retrieved from https://support.avast.com/

Answer Key: Checkpoint 1 - Multiple Choice

1 Mimic Protocol MIMIC — Correct Answer: A

TEACHING NOTE

Mimic protocol wraps connection packets to bypass network firewall filters.

Citation: Mimic Spec [Ref 2].

2 Czech Laws JURISDICTION — Correct Answer: A

TEACHING NOTE

Avast's Czech jurisdiction places it under EU data compliance laws.

Citation: Czech Communications [Ref 3].

3 AES-256 Shield AES-256 — Correct Answer: A

TEACHING NOTE

AES-256 is the standard approved algorithm for securing confidential data.

Citation: AES Standard [Ref 4].

4 Device Links TEN DEVICES — Correct Answer: A

TEACHING NOTE

Avast's multi-device plan allows up to ten simultaneous device link connections.

Citation: Subscription Terms [Ref 5].

5 Session Metrics TIMESTAMPS — Correct Answer: A

TEACHING NOTE

Avast logs connection timestamps and bandwidth data for billing purposes.

Citation: Avast Policy [Ref 1].

Answer Key: Checkpoint 2 - True or False

6 Mimic Protocol — MIMIC BYPASS — Correct Answer: True

TEACHING NOTE

Mimic protocol wraps connection packets to bypass network firewall filters.

Citation: Mimic Spec [Ref 2].

7 Czech Laws — EU COMPLIANCE — Correct Answer: False

TEACHING NOTE

Avast's Czech jurisdiction places it under EU data compliance laws.

Citation: Czech Communications [Ref 3].

8 AES-256 Shield — DATA ENCRYPTION — Correct Answer: True

TEACHING NOTE

AES-256 is the standard approved algorithm for securing confidential data.

Citation: AES Standard [Ref 4].

9 Device Links — MULTI-DEVICE — Correct Answer: False

TEACHING NOTE

Avast's multi-device plan allows up to ten simultaneous device link connections.

Citation: Subscription Terms [Ref 5].

10 Session Metrics — TIMESTAMP LOG — Correct Answer: True

TEACHING NOTE

Avast logs connection timestamps and bandwidth data for billing purposes.

Citation: Avast Policy [Ref 1].

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 MIMIC	B CZECH	C AES256	D TENDEVICES
E TIMESTAMPS	F KILLSWITCH	G PEERTOPEER	H OVERHEAD

CHECKPOINT 3: KEY TERM KEY

1 MIMIC	2 CZECH	3 AES256
4 TENDEVICES	5 TIMESTAMPS	6 KILLSWITCH

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.

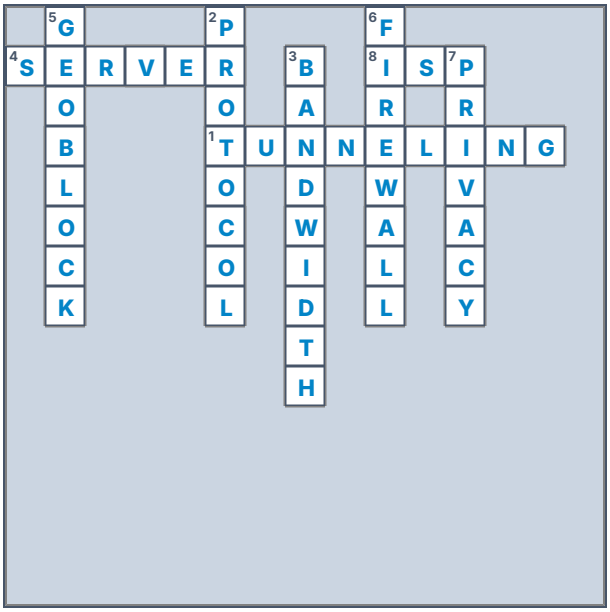
Stealth Representation:
Highlight the role of NDAs and third-party representation in preventing speculative price gouging during corporate procurement.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

CROSSWORD SOLUTION



INSTRUCTOR GUIDE FOR CROSSWORD SOLUTIONS

ACROSS CLUES

1 Across: TUNNELING Process of wrapping data packets. (3,5)

4 Across: SERVER Remote computer routing traffic. (1,0)

8 Across: ISP Internet Service Provider. (1,9)

DOWN CLUES

2 Down: PROTOCOL Rules determining data transmission. (0,5)

3 Down: BANDWIDTH Rate of data transfer. (1,7)

5 Down: GEOBLOCK Location website restriction. (0,1)

6 Down: FIREWALL Security monitor barrier. (0,9)

7 Down: PRIVACY State of freedom from tracking. (1,11)

Scrambled Words & Cipher Solution Key

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

WORD UNSCRAMBLE KEY

1. CMIIM
   MIMIC

2. HCCEZ
   CZECH

3. S652AE
   AES256

4. CEDISVETEN
   TENDEVICES

5. MSTEPMASIT
   TIMESTAMPS

6. TLIWCHISKL
   KILLSWITCH

7. REREOPTEPE
   PEERTOPEER

8. RDVAEOHE
   OVERHEAD

SECRET CIPHER CHALLENGE KEY

"MIMIC PROTOCOL EVADES FIREWALL DETECTION RULES"

VPN & Network Case Studies Solution Key

A Case Study 1: Logging Compliance

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A user reviews Avast's logging policy and notices that while browsing data is not stored, Avast records connection durations and raw bandwidth usage for capacity planning.
- **Recommended Strategy & Solution:** Avast records connection timestamps and raw data volumes during active sessions for capacity management.

B Case Study 2: Firewall Bypass

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** An engineer tries to bypass a network firewall that blocks OpenVPN traffic by scanning packet headers. They need a protocol that disguises VPN packets as standard HTTPS data.
- **Recommended Strategy & Solution:** The engineer should configure the Mimic protocol, which wraps and masks VPN packets to look like standard secure browser requests.