Name: _____ Date: _____ Score: _____

Zero Trust Architecture & Security

Continuous verification, network micro-segmentation, Identity and Access Management, least privilege, and posture checks.

ZERO TRUST SECURITY LEARNING OVERVIEW

SECURED
DATA ENCRYPTION
256-bit AES Standard

COMPLIANT
GLOBAL STANDARDS
GDPR & CCPA Frameworks

ZERO-TRUST
ACCESS POLICY
Multi-Factor Authentication

Welcome! This activity packet guides you through Zero Trust architecture and security. You will explore continuous verification, network micro-segmentation, identity access management (IAM), least privilege, and session auditing.

WORKSHEET CHECKPOINTS

- [ ] **Part 1-4:** Master cybersecurity and threat prevention.
- [ ] **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 Cybersecurity Guide

URL: https://www.vpn.com/cybersecurity/zero-trust-cyber-security/

Your Zero Trust Strategy Learning Roadmap

- Understand the core principle of continuous verification.
- Implement network micro-segmentation and least privilege access.
- Configure device posture checks and active session auditing.

ZERO TRUST 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 Zero Trust architecture.

ZERO TRUST ARCHITECTURE & SECURITY (INTRODUCTION)

Zero Trust security replaces old network perimeter models with a strict 'never trust, always verify' policy. Implementing micro-segmentation, Identity and Access Management (IAM), least privilege rights, and posture checks blocks lateral threat movement.

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

Checkpoint 1: Multiple Choice Challenge

1 What is the core principle of Zero Trust security?

- A. Never trust, always verify every access request regardless of source
- B. Assuming all traffic inside the corporate firewall is safe
- C. Storing database files without encryption to improve speed
- D. Enforcing email authentication using only SPF records

2 What is network micro-segmentation?

- A. Splitting networks into small, isolated zones to contain lateral movement
- B. Encrypting network cards during data transit
- C. Connecting all local servers to a single public IP address
- D. Monitoring user keystrokes in browser sessions

3 What is the principle of least privilege?

- A. Restricting user access permissions to only what is necessary for their job
- B. Giving all system privileges to every user by default
- C. Allowing anonymous logins to corporate database servers
- D. Configuring public Wi-Fi routers without passwords

4 What is Identity and Access Management (IAM)?

- A. Frameworks managing digital identities and controlling system privileges
- B. Antivirus utilities that scan local file directories
- C. A backup storage system using air-gapped media
- D. An email gateway protocol rejecting spoofed domains

5 What does continuous authentication mean?

- A. Repeatedly verifying user identity and device posture during an active session
- B. Changing the master password every 10 minutes
- C. Hashing database records using multiple algorithms
- D. Encrypting network transit packets using TLS keys

Checkpoint 2: True or False Challenge

6 Question 6

Zero Trust assumes that all traffic inside the corporate firewall is safe.

◯ True ◯ False

7 Question 7

Micro-segmentation stops attackers from moving laterally across internal servers.

◯ True ◯ False

8 Question 8

Least privilege grants access to all database files by default.

◯ True ◯ False

9 Question 9

Continuous verification validates device health and credentials throughout a login session.

◯ True ◯ False

10 Question 10

Implementing Zero Trust reduces the impact of compromised corporate logins.

◯ 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. Requiring credentials at every access point is continuous _____.
2. Dividing the corporate network into tiny zones is micro-_____.
3. Configuring digital identities and access control uses an _____ system.
4. Restricting user permissions uses the principle of least _____.
5. Evaluating the health of connected devices scans device _____.
6. Logging and reviewing active sessions is security _____.

VOCABULARY WORD BANK

VERIFICATION	SEGMENTATION	IAM	PRIVILEGE
POSTURE	AUDITING		

Write your answers here:

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

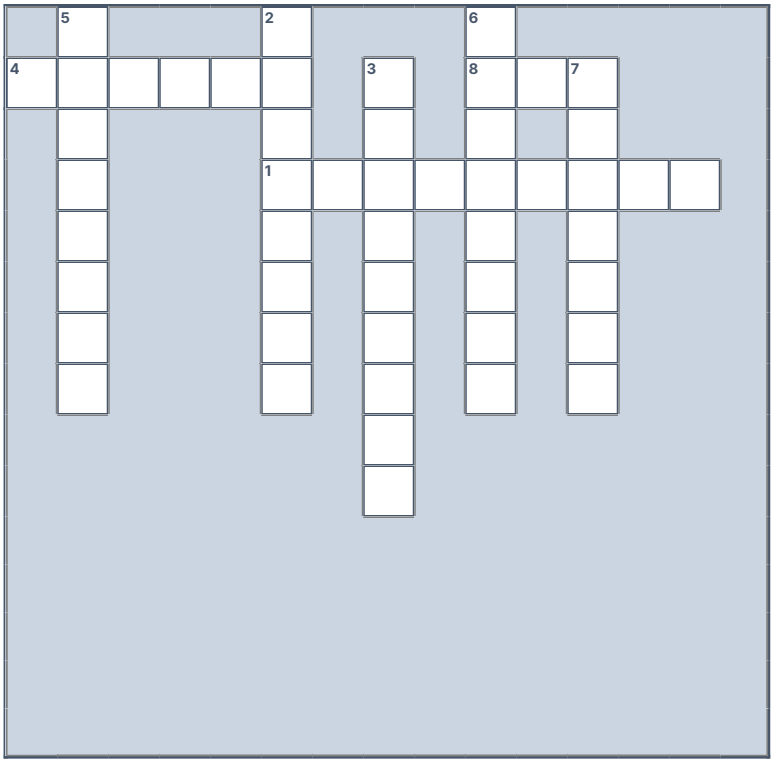
Checkpoint 4: Security Concept Match

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.

VERIFICATION	**A** Always checking user credentials. (A)
SEGMENTATION	**B** Dividing internal network zones. (B)
IAM	**C** Managing user credentials access. (C)
PRIVILEGE	**D** Least access rights principle. (D)
POSTURE	**E** Evaluating device health status. (E)
AUDITING	**F** Reviewing logged access sessions. (F)
FIREWALL	**G** External network barrier protection. (G)
ROUTER	**H** Routing network packet traffic. (H)

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: Continuously authenticating credentials throughout a session. (12 letters):

4 Across: Dividing internal subnets into small department-level zones. (12 letters):

8 Across: Identity framework controlling digital roles and access rights. (3 letters):

DOWN CLUES

2 Down: Restricting user credentials to the absolute minimum needed. (9 letters):

3 Down: Evaluating the security patch status of connecting endpoints. (7 letters):

5 Down: Logging and reviewing network session access histories. (8 letters):

6 Down: Internal gateway monitoring traffic between segmented zones. (8 letters):

7 Down: Physical or logical network node routing packet traffic. (6 letters):

Checkpoint 6: Hidden Word Search

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

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

VOCABULARY WORD LIST

VERIFICATION	SEGMENTATION	IAM	PRIVILEGE
POSTURE	AUDITING	FIREWALL	ROUTER

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. VERIFICATION
B. SEGMENTATION
C. IAM
D. PRIVILEGE
E. POSTURE
F. AUDITING
G. FIREWALL
H. ROUTER

DEFINITIONS & MATCH FIELDS

1. Always checking user credentials.
2. Dividing internal network zones.
3. Managing user credentials access.
4. Least access rights principle.
5. Evaluating device health status.
6. Reviewing logged access sessions.
7. External network barrier protection.
8. Routing network packet traffic.

Checkpoint 7: Scrambled Word Challenge

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

1. N O I T A C I F I R E V

2. N O I T A T N E M G E S

3. M A I

4. E G E L I V I R P

5. E R U T S O P

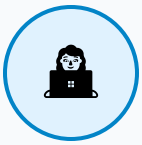
6. G N I T I D U A

7. L L A W E R I F

8. R E T U O R

Checkpoint 8: Cybersecurity Case Studies

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



CASE STUDY 1: TRANSITIONING TO ZERO TRUST NETWORK ARCHITECTURE

Scenario: A large enterprise currently uses a flat internal network where any device on the local network can access all corporate servers and databases.

Discussion Question: Design a network micro-segmentation strategy to limit lateral movement.

CASE STUDY 2: DEPLOYING LEAST PRIVILEGE ACCESS CONTROLS

Scenario: Audit logs reveal that temporary database users and low-level employees hold global read and write permissions to critical accounting databases.

Discussion Question: Audit and restrict database IAM privileges to enforce least privilege.

Final Challenge: Decrypting the Cipher

A cybersecurity professional protects network assets from online threat actors. 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

22 5 18 9 6 25   1 12 23 1 25 19

23 9 20 8   19 5 3 21 18 5   26 5 18 15

20 18 21 19 20   1 18 3 8 9 20 5 3 20 21 18 5

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 Cybersecurity FAQs (Part A)

Review common questions and answers regarding online threat mitigation.

Q1: What is Zero Trust?

Zero Trust is a security framework assuming that threats exist both outside and inside the network boundary, requiring verification for every request.

Q2: What is the core rule of Zero Trust?

Never trust, always verify.

Q3: What is micro-segmentation?

Dividing a network into small, secure logical segments to control traffic and contain breaches.

Q4: What is least privilege?

Giving users only the minimum access rights required to perform their specific work tasks.

Q5: What does IAM stand for?

Identity and Access Management.

Checkpoint 10: Basic Cybersecurity FAQs (Part B)

Review common questions and answers regarding online threat mitigation.

Q6: How does device posture check help?

It verifies that a device is patched, runs active antivirus, and is secure before allowing access.

Q7: What is lateral movement?

The process attackers use to navigate through a network from an initial compromised node to higher-value systems.

Q8: Does Zero Trust replace firewalls?

No, it enhances them by adding identity-centric checks and internal segmentation firewalls.

Q9: What is continuous authentication?

Ongoing verification of user identity throughout an active login session, not just at initial sign-in.

Q10: Why is a flat network dangerous?

In flat networks, a single compromised node allows attackers to easily access any database on the network.

Checkpoint 11: Advanced Security FAQs (Part A)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q1: How does Zero Trust address the perimeter model?

It replaces the outdated 'castle-and-moat' model, shifting defense from boundary networks to specific user identities and resources.

Q2: What is a policy decision point (PDP)?

The system component that evaluates authorization requests against security rules to decide if access should be granted.

Q3: What is a policy enforcement point (PEP)?

The system node (like a gateway or proxy) that physically allows or blocks connection requests based on the PDP decision.

Q4: How does Role-Based Access Control (RBAC) support Zero Trust?

RBAC groups permissions into specific roles, ensuring users do not inherit excessive administrative privileges.

Q5: What is contextual access control?

Evaluating login requests using secondary clues like geographic location, device posture, and login time to assess risk.

Checkpoint 11: Advanced Security FAQs (Part B)

Explore advanced technical aspects of security frameworks, malware analysis, and data compliance.

Q6: How does micro-segmentation differ from standard VLANs?

VLANs divide networks physically, while micro-segmentation uses software firewalls to isolate individual virtual machines and processes.

Q7: What is just-in-time (JIT) access?

Granting elevated administrative permissions temporarily and automatically revoking them once the task is finished.

Q8: How do you secure APIs in a Zero Trust framework?

By requiring cryptographically signed OAuth tokens and auditing request signatures at every API gateway.

Q9: What is a zero-trust network access (ZTNA) client?

A software agent that establishes secure, encrypted outbound connections to specific applications rather than raw network subnets.

Q10: How does log auditing assist Zero Trust?

Continuous logging allows automated security analytics tools to detect anomalies and immediately suspend rogue logins.

Part 11: 10 Real-World Cybersecurity Facts & Insights

Review real-world facts regarding security breaches, defense mechanisms, and compliance standards.

1. SECURITY INSIGHT

Zero Trust architectures replace the legacy castle-and-moat model with identity-centric verification rules.

2. SECURITY INSIGHT

Network micro-segmentation reduces the lateral propagation area of internal malware infections by over 90%.

3. SECURITY INSIGHT

Over 70% of enterprise organizations are actively migrating toward a Zero Trust security framework.

4. SECURITY INSIGHT

Least privilege access policies reduce the risk of insider threat data egress from core databases.

5. SECURITY INSIGHT

Device posture validation checks operating system patch levels and active antivirus state in real time.

6. SECURITY INSIGHT

Zero Trust Network Access (ZTNA) brokers replace traditional corporate VPN networks to restrict user access scope.

7. SECURITY INSIGHT

Just-in-Time (JIT) administrative privilege delegation reduces credential theft risk on domain controllers.

8. SECURITY INSIGHT

Continuous validation logs and audits session behavior, suspending users showing anomalous script execution patterns.

9. SECURITY INSIGHT

Traditional perimeter defenses fail to block lateral attacks once an administrative credential is leaked.

10. SECURITY INSIGHT

NIST Special Publication 800-207 defines the federal standards and architecture rules for Zero Trust deployment.

Technical References & Sources

The study guide and interactive puzzles are compiled from global NIST, OWASP, and data privacy compliance standards.

SCHOLARLY & INDUSTRY REFERENCES

[1] CISA. (2025). Cybersecurity Alerts & Advisories. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories

[2] GDPR. (2024). General Data Protection Regulation (GDPR) Official Text. Retrieved from https://gdpr-info.eu/

[3] NIST. (2024). Special Publication 800-53: Security and Privacy Controls. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[4] NIST. (2023). Special Publication 800-61: Computer Security Incident Handling Guide. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[5] NIST. (2023). Special Publication 800-88: Guidelines for Media Sanitization. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final

[6] IETF. (2021). RFC 8446: Transport Layer Security (TLS) 1.3 Specification. Retrieved from https://datatracker.ietf.org/doc/rfc8446/

[7] IETF. (2022). RFC 7519: JSON Web Token (JWT) Specification. Retrieved from https://datatracker.ietf.org/doc/rfc7519/

[8] Center for Internet Security (CIS). (2024). Critical Security Controls. Retrieved from https://www.cisecurity.org/controls/cis-controls-list

[9] OWASP. (2024). Top 10 Web Application Security Risks. Retrieved from https://owasp.org/www-project-top-ten/

[10] OWASP. (2025). Application Security Verification Standard (ASVS). Retrieved from https://owasp.org/www-project-application-security-verification-standard/

Answer Key: Checkpoint 1 - Multiple Choice

1 Brokerage Function

BROKERAGE

Correct Answer: A

TEACHING NOTE

Domain brokers act as confidential negotiators representing buyers and sellers to reach fair market transactions.

Citation: ICANN Transfer Policy [Ref 1].

2 Stealth Strategy

STEALTH

Correct Answer: A

TEACHING NOTE

Stealth acquisition conceals corporate buyer identity to prevent sellers from inflating asking prices.

Citation: Escrow.com Protocol [Ref 7].

3 Escrow Protection

ESCROW

Correct Answer: A

TEACHING NOTE

Licensed third-party escrow holds funds safely until ownership transfer verification is complete.

Citation: Escrow.com Protocol [Ref 7].

4 Domain Appraisal

VALUATION

Correct Answer: A

TEACHING NOTE

Short 2-letter and 1-word .com domains carry extreme global brand scarcity and liquidity.

Citation: WIPO UDRP Guide [Ref 3].

5 Dispute Resolution

UDRP POLICY

Correct Answer: A

TEACHING NOTE

ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) governs administrative trademark disputes.

Citation: WIPO Dispute Rules [Ref 2].

Answer Key: Checkpoint 2 - True or False

6 Confidential NDAs NDAS — Correct Answer: False

TEACHING NOTE

Professional domain brokers operate under non-disclosure agreements to protect buyer corporate strategy.

Citation: CIS Controls [Ref 8].

7 Escrow Delivery ESCROW — Correct Answer: True

TEACHING NOTE

Escrow holding accounts disburse funds only after full domain ownership transfer is verified by the buyer.

Citation: Escrow.com Protocol [Ref 7].

8 Digital Real Estate ASSETS — Correct Answer: False

TEACHING NOTE

Short 2-letter and 3-letter .com domains function as high-value, liquid digital property assets.

Citation: NIST Guidelines [Ref 9].

9 Stealth Negotiation STRATEGY — Correct Answer: True

TEACHING NOTE

Direct corporate buyer outreach often causes sellers to inflate asking prices significantly.

Citation: WIPO UDRP Guide [Ref 3].

10 EPP Authorization EPP CODE — Correct Answer: True

TEACHING NOTE

EPP codes are unique security passcodes generated by registrars to authorize domain transfers.

Citation: IETF RFC 5730 [Ref 4].

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 VERIFICATION	B SEGMENTATION	C IAM	D PRIVILEGE
E POSTURE	F AUDITING	G FIREWALL	H ROUTER

CHECKPOINT 3: KEY TERM KEY

1 VERIFICATION	2 SEGMENTATION	3 IAM
4 PRIVILEGE	5 POSTURE	6 AUDITING

DISCUSSION NOTES FOR INSTRUCTORS

Threat Landscape:
Verify that students understand how malware, phishing, and zero-day attacks target and disrupt network defenses.

Defense Controls:
Emphasize the deployment of network firewalls, sandbox execution, behavior scanners, and multi-factor authentication (MFA).

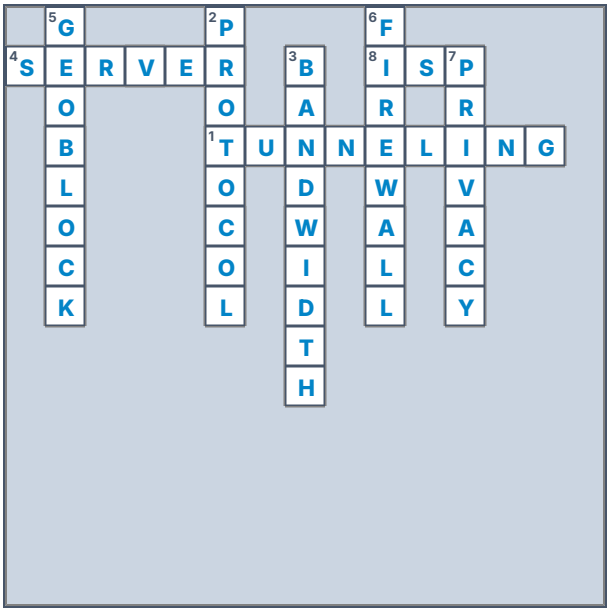
Regulatory Compliance:
Highlight user consent, data minimization, encryption at-rest and in-transit, and global frameworks like GDPR/CCPA.

Puzzles Keys & Instructor Notes

WORD SEARCH SOLUTION

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

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. N O I T A C I F I R E V
   VERIFICATION

2. N O I T A T N E M G E S
   SEGMENTATION

3. M A I
   IAM

4. E G E L I V I R P
   PRIVILEGE

5. E R U T S O P
   POSTURE

6. G N I T I D U A
   AUDITING

7. L L A W E R I F
   FIREWALL

8. R E T U O R
   ROUTER

SECRET CIPHER CHALLENGE KEY

"VERIFY ALWAYS WITH SECURE ZERO TRUST ARCHITECTURE"

Domain Brokerage Case Studies Solution Key

A Case Study 1: Transitioning to Zero Trust Network Architecture

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** A large enterprise currently uses a flat internal network where any device on the local network can access all corporate servers and databases.
- **Recommended Strategy & Solution:** Segment the flat network into isolated departmental zones. Install internal firewalls to control traffic between zones, and mandate connection token validation for all access.

B Case Study 2: Deploying Least Privilege Access Controls

Instructor Solution

GRADING GUIDELINE

Student answers should cover the following points:

- **Scenario Analysis:** Audit logs reveal that temporary database users and low-level employees hold global read and write permissions to critical accounting databases.
- **Recommended Strategy & Solution:** Revoke all global administrative privileges. Implement Role-Based Access Control (RBAC) to match exact job roles, and establish weekly automated permission reviews.