Zscaler ZTCA Practice Questions

Shared by Potts on 21-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A Zero Trust solution must account for an enterprise's risk tolerance via:

Options:

A- Industry analyst firms such as Gartner and Forrester should provide the best guidance.
B- A Zero Trust certification process, whereby every employee at the company is Zero Trust certified.
C- A dynamic risk score, which feeds into a decision engine that determines whether access should be granted.
D- The enterprise security architecture team should create a standard formula to calculate a fixed risk score for each unique initiator based on previous security incidents.

Answer:

C

Explanation:

The correct answer is C. In Zero Trust architecture, enterprise risk tolerance is reflected through dynamic assessment, not static trust assumptions. A Zero Trust platform continuously evaluates the context of each request and uses that context to determine the appropriate access outcome. This aligns with the architectural principle that trust is never permanent and should be calculated based on current conditions rather than on a one-time decision or a fixed historical score.

A dynamic risk score is therefore the best fit because it can incorporate changing factors such as user identity, device posture, location, behavior, application sensitivity, and other contextual or security signals. That score then informs a decision engine, which determines whether the request should be allowed, restricted, isolated, deceived, or blocked. This is far more aligned to Zero Trust than depending on analyst advice, employee certification, or a fixed formula based only on earlier incidents.

The key principle is that Zero Trust must adapt to changing risk in real time. Since enterprise risk tolerance varies by application, data sensitivity, and business context, a dynamic scoring and policy decision model is the most accurate architectural answer.

Question 2

Question Type: MultipleChoice

What is policy enforcement with a Zero Trust solution?

Options:

A- Access control delivered via authentication, authorization, and accounting through a protocol such as RADIUS.
B- SCIM, leveraging an IdP.
C- Placing virtual firewall images in every public cloud you are deployed in.
D- The unique and definitive implementation of control, solely for that access request.

Answer:

D

Explanation:

The correct answer is D. In Zero Trust architecture, policy enforcement is the specific control decision applied to a particular access request, based on the exact context of that request at that moment. Zscaler's architecture guidance emphasizes granular, context-based policies that control application access independently of IP address or location. It also explains that policy is determined by evaluating the user, device, location, group, and other factors, which means enforcement is transaction-specific rather than a broad network permission.

Option A refers to traditional AAA concepts and protocols, which may participate in identity workflows but do not define Zero Trust policy enforcement by themselves. Option B, SCIM with an Identity Provider (IdP), relates to identity provisioning rather than runtime enforcement. Option C reflects a legacy or infrastructure-centric design pattern, not Zero Trust. In contrast, Zero Trust enforcement is the actual outcome applied to that single request, such as allow, restrict, isolate, deceive, or block, depending on verified context. This is why the best answer is that policy enforcement is the unique and definitive implementation of control solely for that access request, not a generalized network-level permission model.

Question 3

Question Type: MultipleChoice

Content stored within a SaaS/PaaS/IaaS location can be:

Options:

A- 100% trusted, as cloud providers make sure content is safe before it is uploaded.
B- Considered risky until inspected, either through inline SSL/TLS controls or through assessing the files ''at rest'' using an out-of-band assessment.
C- Partially trusted depending on whether you maintain a proper audit log for access.
D- Should never be trusted.

Answer:

B

Explanation:

The correct answer is B. In Zero Trust architecture, content stored in Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS) environments should not be assumed safe simply because it resides in a cloud platform. Zscaler's security model emphasizes that trust must be established through inspection and policy, not by location alone. The TLS/SSL inspection architecture shows that inline inspection is necessary to evaluate content moving through encrypted sessions, while Zscaler's broader data protection model also includes out-of-band assessment for content already stored in cloud services.

This aligns with the Zero Trust principle that applications and content can exist anywhere, but they are not automatically trustworthy because of where they are hosted. Cloud providers secure the platform, but they do not guarantee that every uploaded file, shared object, or stored dataset is safe, compliant, or free from malware or data exposure risk. At the same time, saying content should never be trusted is too absolute; Zero Trust is about verification, not blanket denial. Therefore, the most accurate answer is that cloud-stored content should be treated as risky until inspected, whether inline during transfer or out of band while at rest.

Question 4

Question Type: MultipleChoice

A Zero Trust solution must account for an enterprise's risk tolerance via:

Options:

A- Industry analyst firms such as Gartner and Forrester should provide the best guidance.
B- A Zero Trust certification process, whereby every employee at the company is Zero Trust certified.
C- A dynamic risk score, which feeds into a decision engine that determines whether access should be granted.
D- The enterprise security architecture team should create a standard formula to calculate a fixed risk score for each unique initiator based on previous security incidents.

Answer:

C

Explanation:

The correct answer is C. In Zero Trust architecture, enterprise risk tolerance is reflected through dynamic assessment, not static trust assumptions. A Zero Trust platform continuously evaluates the context of each request and uses that context to determine the appropriate access outcome. This aligns with the architectural principle that trust is never permanent and should be calculated based on current conditions rather than on a one-time decision or a fixed historical score.

A dynamic risk score is therefore the best fit because it can incorporate changing factors such as user identity, device posture, location, behavior, application sensitivity, and other contextual or security signals. That score then informs a decision engine, which determines whether the request should be allowed, restricted, isolated, deceived, or blocked. This is far more aligned to Zero Trust than depending on analyst advice, employee certification, or a fixed formula based only on earlier incidents.

The key principle is that Zero Trust must adapt to changing risk in real time. Since enterprise risk tolerance varies by application, data sensitivity, and business context, a dynamic scoring and policy decision model is the most accurate architectural answer.

Question 5

Question Type: MultipleChoice

Verification of user and device identity is to be enabled for:

Options:

A- Any person who wants to connect to an enterprise-controlled application, including employees, third parties, and partners.
B- Remote employees only.
C- Untrusted third parties only.
D- Employees connecting from unmanaged endpoint devices only.

Answer:

A

Explanation:

The correct answer is A. In Zero Trust architecture, verification of both user identity and device context should be applied to any person requesting access to an enterprise-controlled application. That includes employees, contractors, partners, and other third parties. Zscaler's Universal ZTNA guidance states that Zero Trust gives users access to applications based on granular, context-based policies and that the user can be anywhere while the application can be hosted anywhere. This model is not restricted only to remote employees or only to outside parties.

The central principle is that no category of user receives automatic trust simply because of employment status, device ownership, or location. Instead, every access request must be evaluated using current identity and contextual information. That is why Zero Trust architectures verify not just the individual but also conditions such as device posture, location, group, and other policy-relevant attributes. Restricting this verification only to remote staff, unmanaged devices, or external users would recreate the implicit-trust problem that Zero Trust is meant to eliminate. Therefore, the correct architectural answer is that verification should apply to any person connecting to an enterprise-controlled application.

Question 6

Question Type: MultipleChoice

Assessing, calculating, and delivering a risk score is: (Select 2)

Options:

A- An assessment of inline and out-of-band network traffic.
B- A review of known configuration, and the absence of other configuration details, of cloud-hosted services in relation to best practices, industry standards, and compliance models to ensure misconfigurations, issues, and vulnerabilities are understood and highlighted.
C- An assessment of the content, not just the connection, of services, so that malicious functions are not downloaded and protected information is not lost.
D- Only focused on initiator context.

Answer:

A, B

Explanation:

The correct answers are A and B. In Zero Trust architecture, risk scoring is broader than a

simple connection decision. It is derived from multiple forms of context and telemetry so that policy can adapt based on changing conditions. Option A is correct because risk can be informed by both inline observations and out-of-band analysis. This reflects the Zero Trust principle of continuous assessment rather than one-time trust establishment.

Option B is also correct because modern risk evaluation includes the security posture of cloud-hosted services, including known configuration weaknesses, missing controls, misconfigurations, compliance gaps, and other exposures. This aligns with Zero Trust thinking because access and trust decisions should account for more than identity alone; they should also reflect the security condition of the service being accessed.

Option C describes content inspection and data protection, which are critical controls, but that is not the best definition of calculating and delivering a risk score. Option D is incorrect because Zero Trust risk is not only about initiator context. It also considers application, service, transaction, and environmental conditions. Therefore, the two correct answers are A and B.

P2P exams

Question 7

Question Type: MultipleChoice

A Zero Trust policy enablement and subsequent application connection should always be permanent.

Options:

A- True
B- False

P2P exams

Answer:

B

Explanation:

The correct answer is B. False. Zero Trust architecture is built around least-privileged, context-based access, not permanent entitlement. Zscaler's ZPA guidance explains that ZTNA provides users secure connectivity to private applications without ever placing them on the network and that access is granted based on granular policies. When a user attempts to access a resource, the user's context is matched against policy, and if the requirements are not met, the application is effectively unreachable.

This means access is conditional and specific, not permanently enabled after one successful decision. Zscaler also emphasizes that users connect directly to apps, not the network,

minimizing attack surface and eliminating lateral movement. A permanent connection model would resemble legacy VPN behavior, where a user gains broad, lasting access to a routed network environment. Zero Trust rejects that model. Instead, policy enablement and application connectivity are tied to the active request and the context at the time of access. If posture, location, or policy conditions change, the decision can also change. Therefore, Zero Trust connections should not always be permanent, and the correct answer is False.

Question 8

Question Type: MultipleChoice

What purpose do Data Loss controls serve? (Choose all that apply)

Options:

A- Detecting data theft through malware.
B- Preventing non-malicious and/or accidental data leakage.
C- Error checking and validation to ensure data integrity.
D- Intercepting data poisoning attempts from authorized users.

Answer:

A, B

Explanation:

The correct answers are A and B. In Zero Trust architecture, Data Loss controls exist to prevent sensitive information from leaving the organization in unauthorized ways. Zscaler's TLS/SSL inspection reference architecture specifically lists Data Loss Prevention (DLP) as a capability that helps prevent sensitive data from leaving the organization. This clearly supports option B, which covers accidental or non-malicious leakage such as unintended sharing, upload mistakes, or improper transfers.

Option A is also correct because data loss controls help detect and stop data theft, including theft carried out by malware or compromised sessions. In Zero Trust, inspection is not limited to who is connecting; it also evaluates what content is moving across the session. That is why encrypted traffic inspection is so important: without it, malicious exfiltration can remain hidden. By contrast, option C describes data integrity and validation functions, which are not the purpose of DLP. Option D refers more to content manipulation or poisoning, which is not the primary function being described by data loss controls in Zscaler's architecture. Therefore, the correct purposes are detecting data theft and preventing accidental leakage.

To Get Premium Files for ZTCA Visit

https://www.p2pexams.com/products/ztca

For More Free Questions Visit

https://www.p2pexams.com/zscaler/pdf/ztca

