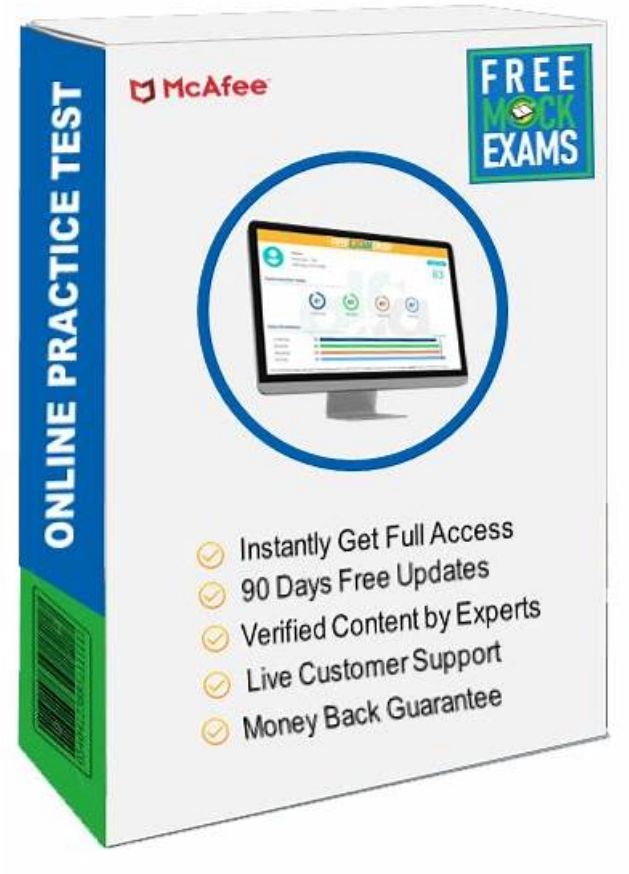
Reliable ZTCA Mock Test - Detailed ZTCA Study Dumps



Zscaler ZTCA exam is an popular examination of the IT industry, and it is also very important. We prepare the best study guide and the best online service specifically for IT professionals to provide a shortcut. TorrentExam Zscaler ZTCA Exam covers all the content of the examination and answers you need to know. Tried Exams ot TorrentExam, you know this is something you do everything possible to want, and it is really perfect for the exam preparation.

Zscaler ZTCA Exam Syllabus Topics:

Topic	Details
Topic 1	• Zero Trust Architecture Deep Dive Introduction: This domain introduces the foundational concepts of Zero Trust Architecture and prepares learners for deeper topics in the course. It provides a high-level understanding of how the Zero Trust framework operates within modern security environments.
Topic 2	• Zero Trust Architecture Deep Dive Summary: This domain provides a recap of the Zero Trust concepts and practices discussed throughout the course. It reinforces the key elements required to successfully design and implement a Zero Trust architecture.
Topic 3	• An Overview of Zero Trust: This section explains the shift from traditional network security models to a Zero Trust architecture. It covers how Zero Trust connections are established and introduces the key principles of verifying identity, controlling content and access, enforcing policy, and securely initiating connections to applications.

Topic 4	• Enforce Policy: This section explains how security policies are applied and enforced across user connections and application access. It focuses on ensuring that access decisions follow defined policies and that connections to applications remain secure and compliant.

Detailed ZTCA Study Dumps | Valid ZTCA Test Questions

Each important section of the syllabus has been given due place in our ZTCA practice braindumps. Hence, you never feel frustrated on any aspect of preparation, staying with our ZTCA learning guide. Every ZTCA exam question included in the versions of the PDF, SORTWARE and APP online is verified, updated and approved by the experts. With these outstanding features of our ZTCA Training Materials, you are bound to pass the exam with 100% success guaranteed.

Zscaler Zero Trust Cyber Associate Sample Questions (Q56-Q61):

NEW QUESTION # 56
What purpose do Data Loss controls serve? (Select all that apply)

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

Answer: B,C

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 .

NEW QUESTION # 57
What is the trend that is increasing security risk through legacy solutions that drive network sprawl?

- A. More applications moving to the cloud, users being remote, and VPNs and firewalls extending IP connectivity out to several different locations.
- B. A spread-out group of access control lists (ACLs) and firewall rules, with each firewall and VPN appliance only enforcing a subset of the total rule list.
- C. A desire to replace edge routers with SD-WAN boxes, which can leverage multiple uplinks for active- active VPN failover.
- D. An ongoing dependence on Layer 2 and Layer 3 switching, without consideration for upcoming 5G architectures.

Answer: A

Explanation:
The correct answer is D . Zscaler's Zero Trust architecture specifically contrasts modern distributed environments with legacy VPN- and firewall-based designs. The reference architecture explains that users are now remote, applications can be hosted in public cloud, private cloud, or data centers, and access must work across any location. In legacy models, organizations respond by extending IP connectivity outward through VPNs, firewalls, and other network-based controls. That expansion increases the attack surface, preserves broad network trust, and drives network sprawl instead of reducing it.

The same guidance states that Zero Trust gives users access to applications without ever placing them on the network or exposing apps to the internet . This is important because legacy architectures extended the organizational perimeter to end users, allowing lateral movement and increasing risk when users and apps became more distributed. Option A describes a symptom of legacy complexity, but option D captures the broader trend that is causing the sprawl in the first place: cloud migration, remote users, and the continued use of VPN and firewall architectures to maintain connectivity. That is the most accurate Zero Trust answer.

NEW QUESTION # 58
What is a security limitation of traditional firewall/VPN products?

- A. Their IP addresses are published on the internet.
- B. SSL-encrypted VPN traffic bypasses security inspection.
- C. They rely on easily tampered-with endpoint software.
- D. They cannot be scaled to handle increased load.

Answer: B

Explanation:
The correct answer is B. A key limitation of many traditional firewall and virtual private network (VPN) architectures is that encrypted VPN traffic can bypass or reduce effective security inspection, especially when the architecture is designed mainly to provide network connectivity rather than full inline content inspection.
Zscaler's TLS/SSL inspection guidance explains that without decryption, organizations are limited in how well they can inspect content for malware, data exfiltration, and risky activity. It also notes that legacy platforms often struggle to inspect encrypted traffic at scale, which creates blind spots in protection.
This matters because Zero Trust is not satisfied by simply creating a secure tunnel. A tunnel can protect confidentiality in transit, but it does not guarantee that the content inside the connection is safe or compliant.
Zscaler's Zero Trust architecture shifts away from broad network access and toward inline, policy-driven inspection and enforcement. The issue is not merely internet publication of IPs or scalability in the abstract; the deeper security weakness is that encrypted traffic can traverse the legacy VPN model without full security visibility and control.

NEW QUESTION # 59
Verification of user and device identity is to be enabled for:

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

Answer: C

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.

NEW QUESTION # 60
What protects Personally Identifiable Information (PII) accidentally shared by a colleague to the entire company?

- A. Virtual firewalls.
- B. SSL/TLS inspection.

- C. Verifying identity and context through a secure identity provider.
- D. Data Loss Prevention (out-of-band and inline).

Answer: D

Explanation:
The correct answer is C. Data Loss Prevention (out-of-band and inline). In Zero Trust architecture, protection of sensitive data such as Personally Identifiable Information (PII) is handled by controls that understand and govern the content being transmitted, not just the identity of the sender or the existence of a connection. Zscaler's TLS/SSL inspection reference architecture explicitly identifies Data Loss Prevention (DLP) as a capability that helps prevent sensitive data from leaving the organization . That directly addresses accidental broad sharing, because DLP policies can detect sensitive patterns and stop, restrict, or alert on improper distribution. SSL/TLS inspection helps make the content visible, but by itself it is not the control that decides whether the sensitive information should be allowed. Identity verification is important for access decisions, but it does not prevent a legitimate user from unintentionally oversharing data. Virtual firewalls also do not provide content- aware protection for PII leakage. Zero Trust requires content-aware controls in addition to identity and context, which is why inline and out-of-band DLP is the correct answer for protecting accidentally shared PII.

NEW QUESTION # 61
.....