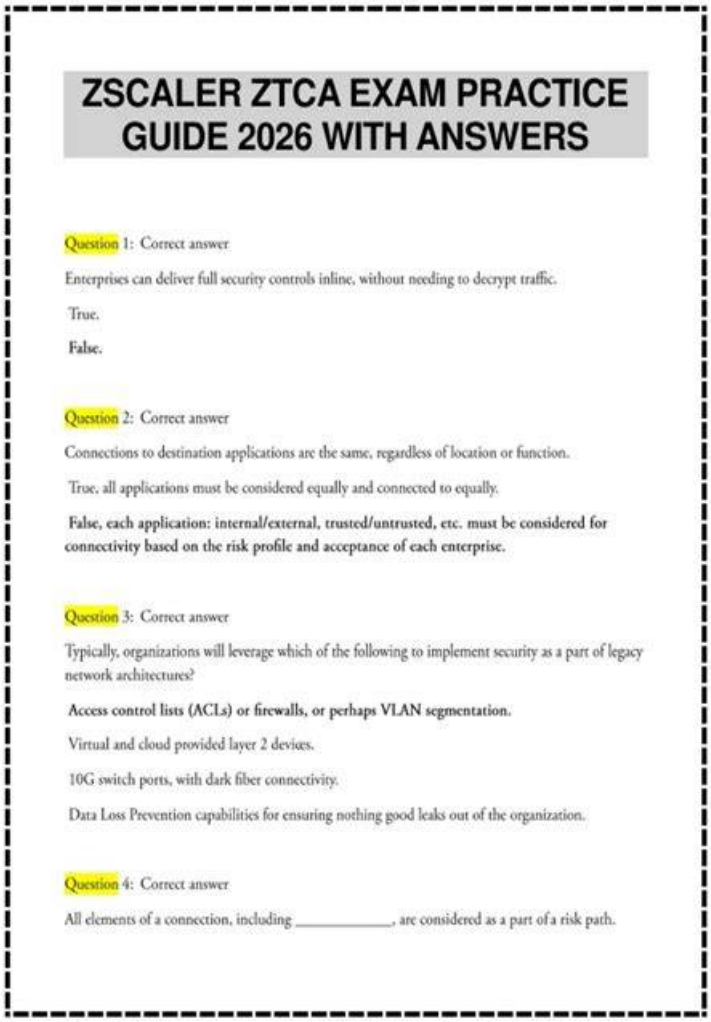
Zscaler ZTCA Trustworthy Practice | Sample ZTCA Test Online


ZSCALER ZTCA EXAM PRACTICE GUIDE 2026 WITH ANSWERS

Question 1: Correct answer

Enterprises can deliver full security controls inline, without needing to decrypt traffic.

True.

False.

Question 2: Correct answer

Connections to destination applications are the same, regardless of location or function.

True, all applications must be considered equally and connected to equally.

False, each application: internal/external, trusted/untrusted, etc. must be considered for connectivity based on the risk profile and acceptance of each enterprise.

Question 3: Correct answer

Typically, organizations will leverage which of the following to implement security as a part of legacy network architectures?

Access control lists (ACLs) or firewalls, or perhaps VLAN segmentation.

Virtual and cloud provided layer 2 devices.

10G switch ports, with dark fiber connectivity.

Data Loss Prevention capabilities for ensuring nothing good leaks out of the organization.

Question 4: Correct answer

All elements of a connection, including _____, are considered as a part of a risk path.

We take the leader position in the career of assisting the candidates in passing their ZTCA exams and gaining their dreaming certifications. On the way to be successful, a large number of the candidates feel upset or disturbed when they study with the books or other ZTCA Exam Materials. With our high pass rate as 98% to 100%, which is provided and tested by our worthy customers, you will be encouraged to overcome the lack of confidence and establish your determination to pass ZTCA exam.

Zscaler ZTCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Verify Identity and Context: This section focuses on validating who is connecting, understanding the access context, and determining where the connection is going. It highlights architectural best practices and explains how identity and contextual information are used to secure connections within a Zero Trust ecosystem.

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.

>> Zscaler ZTCA Trustworthy Practice <<

Sample ZTCA Test Online - Actual ZTCA Test Answers

May be you will meet some difficult or problems when you prepare for your ZTCA exam, you even want to give it up. That is why I suggest that you must try our study materials. Because ZTCA guide torrent can help you to solve all the problems encountered in the learning process, ZTCA Study Tool will provide you with very flexible learning time so that you can easily pass the exam. I believe that after you try our products, you will love it soon.

Zscaler Zero Trust Cyber Associate Sample Questions (Q50-Q55):

NEW QUESTION # 50
Should policy enforcement apply to all traffic, including from authorized initiators?

- A. Zero Trust allows all initiators to see the destination, regardless of role and responsibility.
- B. Unauthorized initiators are blackholed by default.
- C. A true Zero Trust solution must never allow any access without authorization.
- D. No. It should only apply to unauthorized initiators.

Answer: C

Explanation:
The correct answer is A . In Zero Trust architecture, policy enforcement applies to every access request , including requests from users who may ultimately be authorized. Zscaler documentation explains that when a user requests access, the platform evaluates context such as identity, posture, location, group membership, and application conditions , then enforces the matching policy. This means that authorized users are not exempt from policy; rather, policy is what determines whether they are authorized for that specific request.
ZPA guidance also states that access policies use explicit logic based on application segments, SAML attributes, client type, and posture profiles, and that traffic that does not match a policy is automatically blocked . This is fully consistent with the principle that no access should occur outside authorization and policy control.
Option A is the only choice that matches that Zero Trust principle, even though its wording is broader than the question. Options B, C, and D are incorrect because they either exclude authorized users from enforcement or imply unnecessary visibility to destinations. In Zero Trust, all traffic is subject to policy , and nothing should be allowed without authorization.

NEW QUESTION # 51
Is risk the same across users?

- A. No.
- B. Yes.

Answer: A

Explanation:
The correct answer is B. No. In Zero Trust architecture, risk is not uniform across users . Zscaler guidance explains that policy and access decisions are based on the entire user context , including identity, device, location, compliance state, and other factors. The same user can even receive different access outcomes depending on whether they are on a corporate laptop at a branch office or on a personal phone at a coffee shop.
This means risk is dynamic and personalized. One user may be low risk because they are on a managed, compliant endpoint in a trusted environment. Another user may be higher risk because they are using an unmanaged device, showing risky behavior, or requesting access to a more sensitive application. Zero Trust depends on this variation. If risk were identical across all users, there would be no need for granular policies, posture checks, or context-aware enforcement.
Therefore, Zero Trust assumes that risk changes by user, device, session, location, and requested application.

That is why access policy is evaluated per request rather than applied as a one-size-fits-all model. The correct answer is No .

NEW QUESTION # 52
What is the trend that is increasing security risk through legacy solutions that drive network sprawl?

- A. 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.
- B. An ongoing dependence on Layer 2 and Layer 3 switching, without consideration for upcoming 5G architectures.
- C. A desire to replace edge routers with SD-WAN boxes, which can leverage multiple uplinks for active- active VPN failover.
- D. More applications moving to the cloud, users being remote, and VPNs and firewalls extending IP connectivity out to several different locations.

Answer: D

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 # 53
The Zscaler Client Connector is:

- A. A marketplace platform that connects different types of business clients to each other.
- B. An agent installed on the endpoint to tunnel authorized user traffic to the Zero Trust Exchange for protection of SaaS, private applications, and internet-bound traffic.
- C. A device used to create a secure communication channel with a Web Application Firewall (WAF).
- D. A cloud-managed endpoint device via an MDM solution.

Answer: B

Explanation:
The correct answer is C . Zscaler documentation describes Zscaler Client Connector as a lightweight software agent that runs on the endpoint and connects user devices to Zscaler cloud-hosted services. It enables protection for internet destinations through ZIA , access to private applications through ZPA , and visibility through ZDX . The secure mobile access reference architecture states that Zscaler Client Connector connects users and devices to the Zscaler Zero Trust Exchange and enables secure access to the internet and private applications from any location.
This directly matches the description in option C. The agent tunnels or redirects the user's authorized traffic to the Zero Trust Exchange, where security policy and access controls are enforced. It is not a WAF device, not an endpoint itself, and not a marketplace platform. The ZPA troubleshooting guide also notes that the initial request to a private application is initiated from Zscaler Client Connector, which intercepts the application request and forwards it appropriately for policy evaluation and brokering. Therefore, the correct definition is that Zscaler Client Connector is an endpoint agent that securely tunnels authorized user traffic to the Zero Trust Exchange .

NEW QUESTION # 54
What are some of the outputs of dynamic risk assessment?

- A. A full PCAP of the inline data transfer.
- B. Categories, criteria, and insights pertaining to each access request.
- C. An ML/AI-driven engine analyzing and determining application segments after wildcard domains are established.

- D. A backup and restore configuration process, run manually during a change window.

Answer: B

Explanation:
The correct answer is A . In Zero Trust architecture, dynamic risk assessment produces decision-support outputs that help determine how each access request should be handled. Zscaler's identity and policy guidance explains that policy decisions are made by evaluating factors such as the user, device, location, group, and more to determine which policies apply. This means the output of risk assessment is not a packet capture or an operational maintenance workflow; it is the contextual information used to classify the request and enforce the appropriate control outcome.
This aligns closely with the idea of categories, criteria, and insights attached to an access request.
Categories help classify the transaction or destination, criteria define which conditions are being evaluated, and insights provide the context needed to allow, restrict, deceive, isolate, or block. By contrast, a full PCAP is a troubleshooting artifact, not a core policy output. Backup and restore processes are administrative operations, and ML-based application segmentation is a separate discovery or segmentation capability rather than the direct output of dynamic risk assessment. Therefore, the best Zero Trust answer is that dynamic risk assessment produces contextual outputs tied to each access request so policy enforcement can be precise and adaptive.

NEW QUESTION # 55
.....