What Will be the Result of Preparing with Zscaler ZTCA Practice Questions?

BTW, DOWNLOAD part of Dumpkiller ZTCA dumps from Cloud Storage: https://drive.google.com/open?id=1ha0FgNWvjAjMd2PElohJprWO_jIbhn4d

As far as the Zscaler Zero Trust Cyber Associate (ZTCA) exam questions are concerned, these Zscaler ZTCA exam questions are designed and verified by the experience and qualified ZTCA exam trainers. They work together and strive hard to maintain the top standard of ZTCA Exam Practice questions all the time. So you rest assured that with the Dumpkiller Zscaler ZTCA exam questions you will ace your ZTCA exam preparation and feel confident to solve all questions in the final Zscaler ZTCA exam.

Zscaler ZTCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• 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.
Topic 4	• 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 5	• Control Content & Access: This domain covers how organizations assess risk, prevent compromise, and protect sensitive data when users access applications or services. It emphasizes adaptive controls, security inspection, and data protection practices aligned with Zero Trust principles.

>> Reliable ZTCA Exam Cost <<

2026 Latest ZTCA – 100% Free Reliable Exam Cost | Guaranteed Zscaler Zero Trust Cyber Associate Passing

As is known to all, before purchasing the ZTCA Study Guide, we need to know the features of it. We offer you free demo to have a try, so that you can know the characteristics of ZTCA exam dumps. Beside we have three versions, each version have its own advantages, and they can meet all of your demands. And we have free update for 365 days after buying, the latest version will send to you email box automatically.

Zscaler Zero Trust Cyber Associate Sample Questions (Q69-Q74):

NEW QUESTION # 69
What is a security limitation of traditional firewall/VPN products?

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

Answer: C

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 # 70
A Zero Trust network can be:

- A. Built using VPN concentrators.
- B. Located anywhere and built on IPv4 or IPv6.
- C. Built on IPv4 or IPv6.
- D. Located anywhere.

Answer: B

Explanation:
The correct answer is D. Located anywhere and built on IPv4 or IPv6. In Zero Trust architecture, the network and application access model is not tied to a specific physical location, branch, or data center.
Zscaler's Zero Trust guidance emphasizes that users, devices, and applications can be securely connected in any location , which is a core shift away from legacy perimeter-based designs. The architecture is also described as IP independent , meaning policy and access decisions are not fundamentally anchored to traditional network constructs such as fixed addressing or trusted subnets. This is why Zero Trust can operate across modern environments regardless of where workloads reside.
The option about VPN concentrators is incorrect because VPN-based architecture is associated with legacy remote-access models that extend network trust and expose services differently from Zero Trust. In contrast, Zero Trust reduces implicit trust, avoids broad network-level access, and focuses on secure, application-aware connectivity. Therefore, the most complete and accurate answer is that a Zero Trust network can be located anywhere and built on IPv4 or IPv6 , rather than being limited to a legacy transport or perimeter model.

NEW QUESTION # 71
Which crucial step occurs during the "Enforce Policy" stage?

- A. Verification of identity and context of the connection.
- B. The setup of an enterprise SSO or AD server for credential validation.
- C. Connecting an initiator to internal and external applications from the Zero Trust Exchange.

- D. A handshake between the initiator and destination application.

Answer: C

Explanation:
The correct answer is A . In the Zero Trust sequence, Verify Identity and Context happens first, followed by Control Content and Access , and then Enforce Policy . The enforce stage is where the platform applies the policy decision and enables the approved transaction to proceed in the allowed manner. In Zscaler's model, this means the Zero Trust Exchange brokers or permits the connection to the authorized application under the right controls.
Option D is incorrect because verification of identity and context belongs to the earlier Verify stage. Option C is about identity infrastructure setup, not runtime enforcement. Option B may occur at a transport level, but it is not the defining Zero Trust function of the Enforce stage.
The best match is therefore the actual application of the policy outcome: the initiator is connected to the appropriate internal or external application through the Zero Trust Exchange according to policy. This is consistent with Zscaler's architecture, where users, devices, and applications are securely connected through the cloud platform and access is granted only after policy evaluation.

NEW QUESTION # 72
Assessing risk is:

- A. A non-recurring process to determine how to treat requests from a specific initiator for the next 30 days.
- B. An assessment of all things related to the current connection, previous context, and considered on an ongoing basis for future requests, thus allowing for unique and dynamic changes in the consideration of risk.
- C. Universal control across the entire enterprise. Once assessed, risk applies to all traffic from that enterprise.
- D. An ongoing process to verify publicly known bad actor IP addresses.

Answer: B

Explanation:
The correct answer is D . In Zero Trust architecture, risk assessment is continuous and adaptive , not static.
Zscaler documentation states that policy decisions consider far more than a one-time identity check. User access is evaluated using context such as user identity, device posture, location, group membership, and time of day , and those conditions can change between requests. ZPA guidance also states that organizations should use logs to determine which users are accessing which apps, and automatically adapt based on any changes in context .
This directly supports the idea that risk is based on the current connection , informed by previous context , and continually reconsidered for future access attempts. Option A is incorrect because Zero Trust does not create a long-lived 30-day trust decision. Option B is incorrect because risk is not universally applied to all enterprise traffic once assessed. Option C is too narrow, since risk is not limited to checking public bad-IP lists. Instead, Zero Trust risk is dynamic and contextual, enabling policy to change uniquely for each request as conditions evolve. That is why the best answer is D .

NEW QUESTION # 73
One example of accessing different types of services based on a differentiator of identity is:

- A. Connecting to a LAN wirelessly versus through a wired connection.
- B. Relying on a Managed Services Provider (MSP) for day-to-day management of the corporate network.
- C. Having an open-access VPN policy.
- D. Connecting from a browser on an untrusted device versus connecting from a device with a Zscaler Client Connector.

Answer: D

Explanation:
The correct answer is C . In Zero Trust architecture, access is determined not only by who the user is, but also by the context of the device and access method . Zscaler documentation explains that policy assignment evaluates the user, machine, location, group, and more to determine which policies apply. It also states that Zero Trust access decisions can consider device posture and whether access is being requested under trusted or untrusted conditions.
A browser session from an untrusted device and a session from a device running Zscaler Client Connector represent two different identity-and-context states. The user identity may be the same, but the device trust and posture are different, so the available services and the enforcement outcome can differ. This is exactly how Zero Trust should work: access is tailored to the verified context of the request rather than granted broadly through network location. The other options do not represent a meaningful Zero Trust identity differentiator.

An open-access VPN policy is contrary to Zero Trust, wired versus wireless is primarily a network transport distinction, and MSP management is unrelated to the access decision itself. Therefore, the best answer is C .

NEW QUESTION # 74

.....

Free demo for ZTCA learning materials is available, you can try before buying, so that you can have a deeper understanding of what you are going to buy. We also recommend you to have a try before buying. In addition, ZTCA training materials contain both questions and answers, and it's convenient for you to check answers after practicing. ZTCA Exam Dumps cover most of the knowledge points for the exam, and you can have a good command of the knowledge points by using ZTCA exam dumps. We have online and offline chat service, if you have any questions, you can consult us.

Guaranteed ZTCA Passing: https://www.dumpkiller.com/ZTCA_braindumps.html

P.S. Free 2026 Zscaler ZTCA dumps are available on Google Drive shared by Dumpkiller: https://drive.google.com/open?id=1ha0FgNWvjAjMd2PElohJprWO_jIbhn4d