ZTCA Popular Exams - Exams ZTCA Torrent

ZTCA study guide can bring you more than you wanted. After you have used our products, you will certainly have your own experience. Now let's take a look at why a worthy product of your choice is our ZTCA actual exam. Firstly, with a high pass rate of 98% to 100%, you will get the pass guarantee form our ZTCA Practice Engine. Secondly, the price of our ZTCA learning guide is quite favourable than the other websites'.

The contents of ZTCA study materials are all compiled by industry experts based on the examination outlines and industry development trends over the years. And our ZTCA exam guide has its own system and levels of hierarchy, which can make users improve effectively. Our ZTCA learning dumps can simulate the real test environment. After the exam is over, the system also gives the total score and correct answer rate.

>> ZTCA Popular Exams <<

Exams ZTCA Torrent - ZTCA Technical Training

If you fail in the exam with our ZTCA quiz prep we will refund you in full at one time immediately. If only you provide the proof which include the exam proof and the scanning copy or the screenshot of the failure marks we will refund you immediately. If any problems or doubts about our ZTCA exam torrent exist, please contact our customer service personnel online or contact us by mails and we will reply you and solve your doubts immediately. Before you buy our product, you can download and try out it freely so you can have a good understanding of our ZTCA Quiz prep. Please feel safe to purchase our ZTCA exam torrent any time as you like. We provide the best service to the client and hope the client can be satisfied.

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	• 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.
Topic 3	• 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 4	• 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 5	• 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.

Zscaler Zero Trust Cyber Associate Sample Questions (Q33-Q38):

NEW QUESTION # 33
What is the security risk inherent in creating a split tunnel VPN, where some traffic is routed over the VPN tunnel and the rest over a direct internet connection?

- A. The VPN traffic is exempted from any security policies configured on the direct internet uplink router or appliance.
- B. You no longer have the visibility required to make decisions on those traffic flows that are going directly out to the internet.
- C. An issue between the built-in client VPN agent on most modern operating systems and a third-party VPN gateway upstream.
- D. A split ACL list, which means only half the rules will be enforced.

Answer: B

Explanation:
The correct answer is B . The core security risk of a split tunnel VPN is loss of visibility and consistent inspection for the traffic that bypasses the tunnel and goes directly to the internet. Zscaler's Secure Mobile Access reference architecture explains that traditional VPNs backhaul traffic to a central data center for security through a legacy appliance stack, while modern remote work leads to a lack of visibility into what users are accessing and how the network is performing when the organization no longer controls the path. ZIA guidance similarly states that user traffic must be forwarded to the nearest ZIA Service Edge so it can be inspected and either forwarded or blocked according to policy, and that the same authentication and policy should follow the user wherever they are. If some traffic exits directly to the internet outside that enforcement path, the organization loses the visibility and control needed to make reliable policy decisions on those flows.
That is the real Zero Trust concern with split tunneling. It creates blind spots rather than a uniformly enforced security model. Therefore, the best answer is loss of visibility into traffic going directly to the internet .

NEW QUESTION # 34
Third parties that can be integrated at the point of Verifying Identity and Context in the Zero Trust process include:

- A. Web scalers such as GCP, Azure, and AWS, where cloud workloads are typically hosted.
- B. Open-source SIEM tools such as OSSM and the ELK Stack.
- C. IdPs (Identity Providers) such as Okta and PingFederate, which are used for SSO (Single Sign-On).
- D. Data center providers such as Equinix, where customer hardware is typically hosted.

Answer: C

Explanation:
The correct answer is B . In Zscaler's Zero Trust architecture, the Verify Identity and Context stage relies on identity systems that can authenticate users and provide policy-relevant attributes. The ZIA authentication architecture explicitly states that Zscaler partners with leading Identity Providers (IdPs) such as Azure Active Directory, Okta, and PingFederate , and that responses from the IdP can include the user's identity, department, and group membership. Those attributes are then used to decide which policies apply.
The ZPA architecture reinforces the same model by stating that SAML and SCIM attributes such as group membership and role are used in access policy rules, and that additional access context can be provided by the SAML Identity Provider . This makes IdP integration a direct part of verification and context evaluation in the Zero Trust process.
The other options are not the best fit for this stage. SIEM tools support logging and analytics, while cloud and data center providers host workloads rather than acting as identity-verification systems. Therefore, the correct answer is IdPs like Okta and PingFederate
.

NEW QUESTION # 35
How is policy enforcement in Zero Trust done?

- A. Without trust, for example Zero Trust.
- B. Conditionally, in that an allow or a block will have additional controls assigned, for example Allow and isolate, or Block and Deceive.
- C. At the network level, by source IP.
- D. As a binary decision of allow or block.

Answer: B

Explanation:
In Zero Trust architecture, policy enforcement is conditional and context-based , not limited to a simple binary allow-or-block model. Zscaler's reference architectures explain that policy is evaluated using the full user context, including identity, device posture, location, group membership, and other conditions. Access decisions are therefore based on whether specific policy conditions are true, rather than only on static network attributes such as source IP address. For example, the same authenticated user may be allowed access from a managed device at headquarters but denied from an airport, even with the same credentials.
Zscaler documentation also shows that Zero Trust policy can go beyond simple pass or deny outcomes by applying additional controls . In DNS Security and Control, requests can be allowed, blocked, or modified.
In ZIA policy development, Cloud App controls allow more granular outcomes than standard allow/block, such as restricting specific actions, applying quotas, or controlling what a user can do inside an application.
This reflects the Zero Trust principle that enforcement is adaptive, granular, and tied to business and security context rather than network location alone.

NEW QUESTION # 36
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 # 37
The Zscaler Zero Trust Exchange has:

- A. Scalable inspection solutions at 150+ public locations and locally in private locations.
- B. Expanded its scope to try to provide the proof for Fermat's Last Theorem.
- C. Locations in few high-traffic geographic regions.
- D. Inspection controls only in limited core sites.

Answer: A

Explanation:

The correct answer is C . Zscaler's reference architectures consistently describe the Zero Trust Exchange as a globally distributed inline cloud platform operating across more than 150 data centers worldwide . The Traffic Forwarding in ZIA reference architecture states that Zscaler has deployed ZIA Service Edge devices in 150+ data centers around the world , allowing users to connect to the nearest service edge for policy enforcement, TLS/SSL inspection, firewalling, and other security services. This design removes the need for centralized backhauling and supports consistent security regardless of user location.
The option mentioning "limited core sites" is incorrect because the Zscaler model is specifically designed to avoid relying on a small number of centralized inspection points. The option about "few high-traffic regions" is also incorrect for the same reason. In addition, Zscaler architecture supports private service edge deployment models for organizations that require local processing in private environments, extending the Zero Trust Exchange model beyond public cloud service edges. Therefore, the only accurate architecture- aligned answer is that Zscaler provides scalable inspection at 150+ public locations and in private locations where needed .

NEW QUESTION # 38
.....

About the dynamic change of our ZTCA guide quiz, they will send the updates to your mailbox according to the trend of the exam. Besides, we understand you may encounter many problems such as payment or downloading ZTCA practice materials and so on, contact with us, we will be there. Our employees are diligent to deal with your need and willing to do their part 24/7. They always treat customers with courtesy and respect to satisfy your need on our ZTCA Exam Dumps.