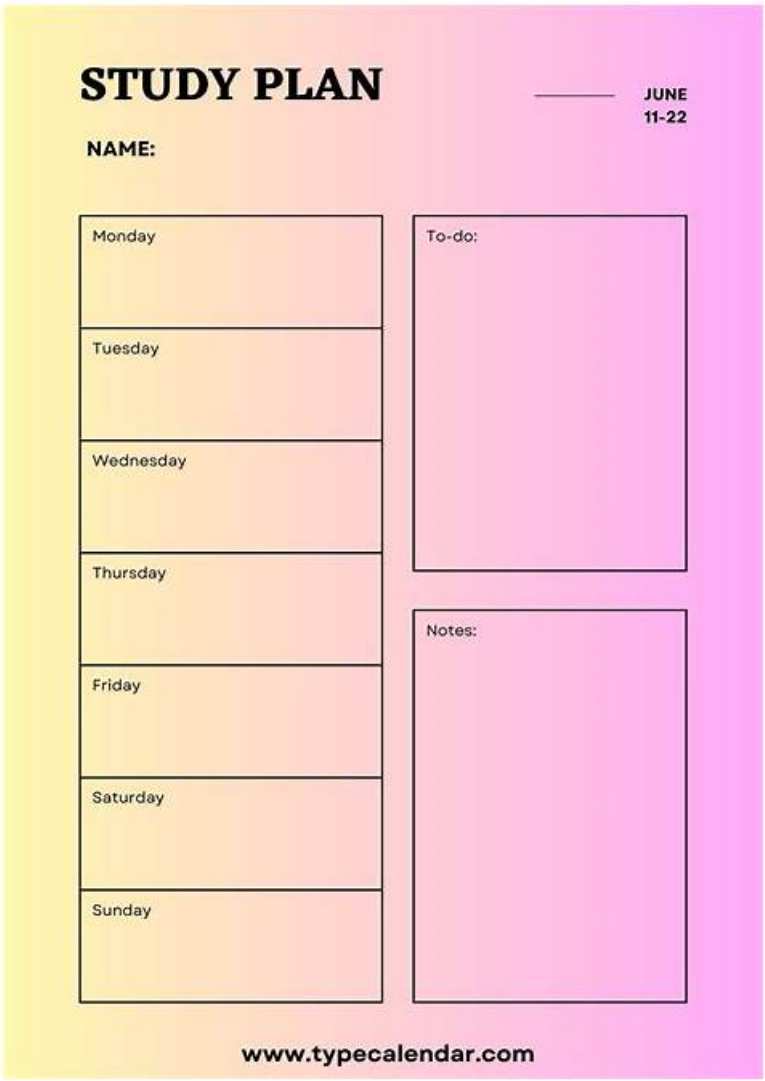
Valid ZTCA Study Plan & New ZTCA Exam Answers



As is known to us, the leading status of the knowledge-based economy has been established progressively. It is more and more important for us to keep pace with the changeable world and improve ourselves for the beautiful life. So the ZTCA certification has also become more and more important for all people. Because a lot of people long to improve themselves and get the decent job. In this circumstance, more and more people will ponder the question how to get the ZTCA Certification successfully in a short time.

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 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 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.

>> Valid ZTCA Study Plan <<

Valid ZTCA test answers & Zscaler ZTCA pass test & ZTCA lead2pass review

If you are preparing the exam, you will save a lot of troubles with the guidance of our ZTCA training engine. Our company is aimed at relieving your pressure from heavy study load. So we strongly advise you to have a try on our ZTCA Study Guide. If you want to know them before your purchase, you can free download the demos of our ZTCA exam braindumps on the website, which are the small part of the learning questions.

Zscaler Zero Trust Cyber Associate Sample Questions (Q72-Q77):

NEW QUESTION # 72
There are alternative traffic forwarding methods to the Client Connector that leverage edge forwarding protocols to connect sites to the Zero Trust Exchange. Two of these protocols are:

- A. Single Sign-On and Public Cloud Access.
- B. Security Appliance and Router.
- C. IPSec and IKEv2.
- D. IPSec and GRE.

Answer: D

Explanation:
The correct answer is A. IPSec and GRE. In the Zscaler Internet Access (ZIA) traffic forwarding architecture, branch offices and sites can send traffic to the Zero Trust Exchange through several forwarding methods. The reference architecture explicitly identifies GRE tunnels and IPsec tunnels as supported methods for forwarding traffic from branch routers, SD-WAN devices, and similar site infrastructure to the nearest ZIA Service Edge.
This is different from Client Connector , which is typically used for individual endpoints such as laptops and mobile devices. For fixed locations, edge-based forwarding protocols are preferred because they allow the site' s egress traffic to be securely transported to Zscaler without requiring the endpoint client on every device. The other options are incorrect because Single Sign-On is an identity function, not a traffic forwarding protocol; Security Appliance and Router are device categories, not protocols; and IKEv2 is associated with IPsec negotiation rather than being presented here as the pair of branch forwarding methods in the ZIA architecture.
Therefore, the two protocols specifically called out as alternative forwarding methods to Client Connector are IPSec and GRE .

NEW QUESTION # 73
The Zscaler Zero Trust Exchange has:

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

Answer: D

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 # 74
Why have traditional networks relied on implicit trust to connect initiators to workloads?

- A. Layer 3 ACLs are sufficient for blocking untrusted initiators.
- B. It was easier to create direct P2P links between all devices, providing connectivity for rapid- downloading applications like BitTorrent and file sharing.
- C. Security breaches were historically less frequent.
- D. TCP/IP, the foundation of most networks, inherently favors connectivity over trust.

Answer: D

Explanation:
The correct answer is B . Traditional networks have historically relied on implicit trust because the foundational model of TCP/IP networking is built to enable connectivity , not to establish trust or least- privileged access. Once a user or device is on the network, routing and addressing make it possible to reach other resources unless additional controls are layered on top. This is exactly the legacy pattern that Zero Trust seeks to replace.
Zscaler's Universal ZTNA guidance explains that legacy approaches connected users to applications by placing them in the same network context or routing domain , whereas Zero Trust decouples the user from the network and allows access only to approved applications. The architecture specifically states that users should access applications without sharing network context with them and that granular, context-based policy should control access instead of implicit network trust.
So the underlying reason is architectural: traditional networking protocols were optimized for reachability and communication, not identity-based trust decisions. That is why implicit trust became common, and why Zero Trust is such a significant shift away from the old model.

NEW QUESTION # 75
What protects Personally Identifiable Information (PII) accidentally shared by a colleague to the entire company?

- A. SSL/TLS inspection.
- B. Virtual firewalls.
- 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 # 76
Policy enforcement in Zero Trust is assessed:

- A. Only if the risk score is high.
- B. For all traffic from the initiating source.
- C. For authorized users only.
- D. For every access request.

Answer: D

Explanation:
The correct answer is D. For every access request. Zero Trust architecture does not assume that a user, device, or session remains trusted after an initial decision. Instead, access is evaluated request by request , using current identity and contextual information. Zscaler's ZPA guidance explains that when a user authenticates, context such as location, device posture, user group, department, and time of day is evaluated, and when the user attempts to access a resource, that context is matched against policy to determine whether access should be allowed.
ZIA guidance reinforces the same principle by stating that policy assignment evaluates the user, device, location, group, and more to determine which policies apply. That means policy enforcement is not limited to high-risk sessions, nor is it applied only once to all future traffic from a source. It is also not restricted only to already authorized users, because the authorization decision itself is part of the evaluation. In Zero Trust, each access request is independently assessed and enforced according to current policy and context. That is why the best answer is for every access request .

NEW QUESTION # 77
.....