KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **ZTCA**

Title : Zscaler Zero Trust Cyber Associate

Version : DEMO

1.The only way to deploy inspection is to inspect all traffic. Technically speaking, at an architectural level, there is no way to have exceptions, such as for certain websites or for certain types of applications.
A. True
B. False
Answer: B
Explanation:
This statement is false. In Zscaler's Zero Trust architecture, the recommended design objective is to inspect as much encrypted traffic as possible because inspection enables security controls such as malware protection, sandboxing, intrusion prevention system (IPS), browser isolation, Data Loss Prevention (DLP), cloud application controls, tenancy restrictions, and file type controls. The reference architecture states that inspecting all TLS/SSL traffic provides the fullest visibility and strongest protection across the Zero Trust Exchange. However, the same document also clearly confirms that inspection bypasses are supported in specific circumstances. These documented exceptions include banking and finance destinations, healthcare destinations, business functions that require unencryptable traffic, certificate-pinned applications, and some Microsoft 365 application flows that may not function properly under inspection. Zscaler strongly recommends using bypasses only in extreme circumstances, but it does not say exceptions are architecturally impossible.
Therefore, from a verified Zero Trust design standpoint, full inspection is the preferred security posture, while selective exceptions are still an allowed and documented deployment option.

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

3.A Zero Trust network can be:
A. Located anywhere.

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

4.How are services protected in a legacy scenario when they are discoverable on the public Internet? (Select all that apply)
A. Establishing a DMZ that would include multiple products and services.
B. Dynamic Application Security Testing (DAST).
C. A large security stack including appliances that handle functions like global load balancing, firewalling, DDoS, and more.
D. A web application firewall (WAF) for protecting against DDoS and other botnet style attacks.
Answer: A, C, D
Explanation:
The correct answers are A, C, and D. In a legacy architecture, applications that are exposed and discoverable on the public Internet are usually protected by building a DMZ (demilitarized zone) and placing multiple security technologies in front of the service. This commonly includes a large security stack made up of separate appliances or services for functions such as load balancing, firewalling, distributed denial-of-service (DDoS) protection, and related edge security controls. A web application firewall (WAF) is also a standard protective element in these public-facing designs because it adds inspection and protection for web-based attack patterns and internet-originated abuse.
Option B, DAST, is not a correct answer because Dynamic Application Security Testing is a testing and assessment method, not a live architectural protection control that sits inline to defend exposed services in production. Zero Trust architecture contrasts with this legacy model by removing direct public discoverability and reducing dependence on a complex exposed edge stack. Instead of defending openly exposed applications with layered perimeter tools, Zero Trust aims to make applications less discoverable and access more identity- and policy-driven.

5.Content inspection of encrypted content at scale is widely available on most network-based security platforms, such as firewalls, to deploy.

A. True
B. False
Answer: B
Explanation:
The correct answer is B. False. In Zero Trust architecture, inspection of encrypted traffic is a major requirement because most internet traffic is now encrypted, and threats frequently hide inside TLS/SSL sessions. However, Zscaler's TLS/SSL inspection reference guidance explains that this type of inspection is not widely available at scale on most traditional network-based security platforms. Conventional security appliances typically experience a major reduction in effective traffic-handling capacity when decryption is enabled, which is one of the main reasons many legacy environments only inspect a limited subset of encrypted traffic.
This limitation is important in Zero Trust because selective inspection creates blind spots. If encrypted traffic is not inspected broadly, malware delivery, command-and-control activity, risky application behavior, and data exfiltration can bypass security controls. Zscaler's architecture is designed to move this function to a cloud-delivered inline security model so inspection can occur more consistently and at scale. Therefore, the statement is false because traditional firewalls and similar appliances have historically struggled to provide encrypted content inspection broadly and efficiently enough for modern Zero Trust needs.