Zscaler ZTCA Online Test & Reliable ZTCA Test Objectives

The ExamTorrent is committed to providing the best possible study material to succeed in the Zscaler Zero Trust Cyber Associate (ZTCA) exam. With actual PDF questions, customizable practice exams, and 24/7 support, customers can be confident that they are getting the best possible prep material. The ExamTorrent ZTCA is an excellent choice for anyone looking to advance their career with the certification. Buy Now.

Zscaler ZTCA Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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.

>> Zscaler ZTCA Online Test <<

Useful ZTCA Online Test by ExamTorrent

Candidates can benefit a lot if they can get the certificate of the exam: they can get a better job in a big company, and the wage will also promote. Our ZTCA Training Material will help you to get the certificate easily by provide you the answers and questions. The questions and answers of the practicing materials is correct and the updated one, we will also update the version for you regularly, therefore, you can know the latest changes for the exam.

Zscaler Zero Trust Cyber Associate Sample Questions (Q67-Q72):

NEW QUESTION # 67
In a Zero Trust architecture, should applications that you manage have any exposed inbound listeners?

- A. Yes, allow anyone to connect to the listening service, just like having your website on the internet for anyone to connect with.
- B. Yes, allow all inbound to any service; the firewall will protect the application.
- C. Only allow access to those who share the same network.
- D. Inbound listener ports should only be accessible to those initiators who are allowed access. All other access, and visibility, must be denied.

Answer: D

Explanation:
The correct answer is A . A major principle of Zero Trust architecture is that managed applications should not be broadly discoverable or openly reachable in the way legacy internet-facing services often are. Access should be limited only to explicitly authorized initiators , and all other visibility and reachability should be denied. This reduces attack surface, prevents opportunistic scanning, and limits exposure to exploitation attempts before authentication and policy evaluation occur.
Zero Trust does not assume that a firewall alone is sufficient protection for an exposed application. Instead, it seeks to minimize or eliminate unnecessary public exposure in the first place. Likewise, requiring the user to be on the same network is a legacy network-trust model, not a Zero Trust principle. The correct model is that access is granted only after identity and context are verified and policy allows it .
So while an application may technically listen for approved brokered access, it should not be openly visible to unauthorized users or the general internet. Therefore, the best answer is that inbound access should be available only to permitted initiators , while all other access and visibility are denied.

NEW QUESTION # 68
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. More applications moving to the cloud, users being remote, and VPNs and firewalls extending IP connectivity out to several different locations.
- D. A desire to replace edge routers with SD-WAN boxes, which can leverage multiple uplinks for active- active VPN failover.

Answer: C

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 # 69
Which of the following actions can be included in a conditional "block" policy? (Select 2)

- A. Allow the connection.
- B. Deceive: Direct any malicious attack to a restricted decoy.
- C. Quarantine: Ensure access is stopped and assessed.
- D. Firehose: Send TCP resets to the initiator.

Answer: B,C

Explanation:
The correct answers are A and B . In Zero Trust architecture, policy enforcement is not limited to a plain deny decision. Instead, policy can apply contextual control actions based on the assessed risk of the user, device, session, or application behavior. A conditional block policy is meant to stop or contain malicious or unauthorized activity while also reducing attacker effectiveness. Quarantine fits this model because it stops access and places the session, user, or device into a controlled state for further review or remediation. That aligns with Zero Trust principles of least privilege, continuous assessment, and adaptive response. Deceive also fits because modern Zero Trust protections can misdirect suspicious or malicious activity toward controlled decoy resources, limiting real exposure while improving detection and response. This is consistent with Zscaler architecture language describing inline prevention, deception, and threat isolation as protective controls.
By contrast, Allow the connection is not a block action, and Firehose is not a standard Zero Trust conditional block control in the architecture concepts you are testing against. Therefore, the two correct answers are Quarantine and Deceive.

NEW QUESTION # 70
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. False
- B. True

Answer: A

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.

NEW QUESTION # 71
There can be different types of initiators in a Zero Trust model, including:

- A. IP addresses and port numbers.
- B. Devices, IoT/OT, and workloads.
- C. A walled garden for limiting access to certain IPs.
- D. Known TCP sockets.

Answer: B

Explanation:
The correct answer is B . In Zero Trust architecture, an initiator is not limited to a human user on a laptop. It can include many entity types that request access to a service, application, or data set. These can include managed devices, Internet of Things (IoT) systems, Operational Technology (OT) assets, and application workloads . This reflects the broader Zero Trust principle that trust decisions are applied to all requesting entities, not only to traditional employee endpoints.
This is important because modern enterprises no longer consist only of users on corporate desktops. They also include sensors,

industrial systems, virtual machines, containers, and cloud-hosted workloads that generate access requests. Zero Trust must therefore evaluate the identity and context of these initiators using policy, posture, and risk rather than relying only on network location.
The other options are not correct because IP addresses, ports, and sockets are technical connection details, not the actual initiating entity in the Zero Trust model. A walled garden is also a network design concept, not a type of initiator. Therefore, the best answer is devices, IoT/OT, and workloads .

NEW QUESTION # 72
.....

Our ZTCA exam prep is elaborately compiled and highly efficiently, it will cost you less time and energy, because we shouldn't waste our money on some unless things. The passing rate and the hit rate are also very high, there are thousands of candidates choose to trust our ZTCA guide torrent and they have passed the exam. We provide with candidate so many guarantees that they can purchase our ZTCA Study Materials no worries. So we hope you can have a good understanding of the ZTCA exam torrent we provide, then you can pass you ZTCA exam in your first attempt.