DUMPSARENA

Zscaler Zero Trust Cyber Associate

Zscaler ZTCA

Version Demo

Total Demo Questions: 9

Total Premium Questions: 93

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

What is the ultimate goal of policy enforcement?

A. State a conditional allow or a conditional block.

B. Issue a log that can be interpreted in a modern SOC.

C. Designate an initiator as always trustworthy or always untrustworthy.

D. Track network bandwidth utilization across destination application categories.

ANSWER: A

Explanation:

State a conditional allow or a conditional block. Policy enforcement is the point at which a Zero Trust architecture applies policy to an individual access request and produces an actionable access outcome. Rather than assigning permanent trust to a user, device, or network, Zero Trust evaluates relevant context—such as authenticated identity, device security posture, requested resource, and risk signals—and enforces the resulting decision for that request. The essential purpose is therefore to permit access when policy conditions are satisfied or deny it when they are not.

This conditional decision model supports the Zero Trust principle of continuously verifying access rather than relying on implicit trust based on network location or a prior decision. In a Zscaler deployment, enforcement controls use policy and real-time context to govern access to applications, internet destinations, and data. Telemetry and logs are important outputs that support visibility, investigation, and operations, but the enforcement function itself culminates in applying the access decision. This aligns with the NIST Zero Trust Architecture description of the policy enforcement point, which enables, monitors, and terminates connections according to decisions made by the policy engine. See NIST SP 800-207: Zero Trust Architecture and Zscaler: What Is Zero Trust Architecture?.

QUESTION NO: 2

A security team is designing access for an administrator who uses the same private application as standard employees but can perform privileged actions within it. Why is authentication alone insufficient for the access decision?

A. Authentication does not establish the requested resource, authorization, device posture, or other access context.

B. Authentication is used only to assign an IP address to the endpoint.

C. Authentication permanently removes the need for policy enforcement.

D. Authentication applies only to users accessing SaaS applications.

ANSWER: A

Explanation:

Authentication establishes who is requesting access, but Zero Trust policy must also evaluate the requested application, the user's authorization, device posture, and other relevant context. The administrator's identity does not automatically justify unrestricted access merely because the application is the same one used by standard employees.

This supports least privilege by allowing policy to distinguish between users and sessions with different levels of risk or authorization. Network location alone is likewise insufficient because it does not establish whether the particular request should be permitted.

QUESTION NO: 3

Assessing, calculating, and delivering a risk score is: (Select 2)

A. An assessment of inline and out-of-band network traffic.

B. A review of known configuration, and the absence of other configuration details, of cloud-hosted services in relation to best practices, industry standards, and compliance models to ensure misconfigurations, issues, and vulnerabilities are understood and highlighted.

C. An assessment of the content, not just the connection, of services, so that malicious functions are not downloaded and protected information is not lost.

D. Only focused on initiator context.

ANSWER: A B

Explanation:

Risk scoring in a Zero Trust program is a continuous process that combines multiple sources of security context into an actionable measure of exposure. An assessment of inline and out-of-band network traffic is correct because inline controls can observe and enforce policy during live transactions, while out-of-band telemetry, logs, and historical analysis provide additional evidence about threats, behaviors, and changing conditions. Together, these signals support a risk score that can be updated as the environment changes rather than relying on a one-time decision.

A review of known configuration, and the absence of other configuration details, of cloud-hosted services in relation to best practices, industry standards, and compliance models to ensure misconfigurations, issues, and vulnerabilities are understood and highlighted is also correct. Cloud-service configuration and posture data reveal exposure that may not be visible from traffic alone. Comparing discovered settings against established security and compliance baselines helps identify weaknesses and contributes meaningful context to an overall risk calculation. Zscaler describes risk management as using contextual intelligence to prioritize and address cyber risk, while its cloud security posture capabilities identify cloud misconfigurations and compliance issues. See Zscaler Risk360 and Zscaler Cloud Security Posture Management.

QUESTION NO: 4

When connecting to internal applications, something that you manage, what is the right way to implement Zero Trust for inbound connections?

A. Direct access to internal applications must never be allowed. Furthermore, internal applications should never be exposed to any untrusted initiator and thus must be dark. Only authorized users can connect.

B. Allow direct access for on-site initiators and enforce authorization for remote connections.

C. Allow direct access for connections from enterprise-managed devices and enforce authorization for unmanaged devices, on-site or remote.

D. Only allow connections via a secure point-to-point VPN connection.

ANSWER: A

Explanation:

Direct access to internal applications must never be allowed. Furthermore, internal applications should never be exposed to any untrusted initiator and thus must be dark. Only authorized users can connect. This expresses the essential Zero Trust approach for private application access: applications are not placed broadly on the network for initiators to discover and reach. Instead, access is established only after the user and context have been evaluated against policy, and only to the specific application or resource for which access is authorized.

Zscaler Private Access implements this model by connecting authorized users to authorized applications without extending network access to the underlying private network. Application Connectors establish outbound-only connections to the Zscaler cloud, so the application does not require an inbound-facing listener or exposure to the public internet. This reduces the externally visible attack surface while supporting least-privileged, identity- and policy-based access. The “dark” concept is therefore not simply a network hardening preference; it is a core design principle that prevents unauthorized initiators from discovering or directly connecting to private applications. Zscaler describes ZTNA as providing secure access to private applications without placing users on the network, and its Zero Trust Exchange architecture enforces application-level access based on policy. See Zscaler’s ZTNA overview and Zscaler Zero Trust Exchange.

QUESTION NO: 5

A user has successfully authenticated from a managed device and is allowed to use an internal collaboration application. The same user then requests access to a highly sensitive payroll application for which they have no authorization. What is the appropriate Zero Trust policy outcome?

A. Deny access to the payroll application while retaining the authorized collaboration access.

B. Allow the payroll application because the device is managed.

C. Disconnect the user permanently from all applications.

D. Provide a VPN so the user can reach the payroll network segment.

ANSWER: A

Explanation:

The correct outcome is to deny the payroll-application request while retaining access only to the authorized collaboration application. Zero Trust authorization is specific to the initiator, the destination application, and the relevant context. A successful authentication or an existing application session does not create entitlement to every other private resource.

Granting access because the device is managed would rely on an overly broad trust decision. Disconnecting the user from all services may be appropriate only if a separate risk condition requires it, but it is not required merely because one unauthorized application request was made. Providing a VPN would create the broad network access that ZTNA is intended to avoid.

QUESTION NO: 6

Which of the following actions can be included in a conditional “block” policy? (Select 2)

A. Quarantine: Ensure access is stopped and assessed.

B. Deceive: Direct any malicious attack to a restricted decoy.

C. Firehose: Send TCP resets to the initiator.

D. Allow the connection.

ANSWER: A B

Explanation:

“Quarantine: Ensure access is stopped and assessed.” and “Deceive: Direct any malicious attack to a restricted decoy.” are valid conditional block-policy actions because a Zero Trust policy decision can apply an adaptive protective response rather than simply ending a session with a generic deny. Quarantine stops the relevant access path and places the affected activity into a controlled state where it can be assessed, investigated, or remediated. This supports continuous verification and least-privileged access by preventing a potentially risky session from proceeding while preserving the context needed for response.

Deception is also an appropriate protective action when suspicious activity is detected. Redirecting an attacker toward controlled decoy assets keeps production resources out of reach while generating high-confidence telemetry about attacker behavior, techniques, and intent. Zscaler describes deception as using decoys and lures to detect threats and enable response before attackers can reach valuable assets. Together, quarantine and deception provide containment and detection capabilities that align with a conditional block decision in a Zero Trust architecture. See Zscaler’s Deception overview and its Zero Trust Architecture overview.

QUESTION NO: 7

Policy enforcement in Zero Trust is assessed:

A. For all traffic from the initiating source.

B. Only if the risk score is high.

C. For authorized users only.

D. For every access request.

ANSWER: D

Explanation:

For every access request. This reflects the core Zero Trust principle that trust is never implicit or permanently granted based solely on a prior authentication event, network location, or earlier authorization decision. Each attempt to access an application, service, or resource is evaluated against the organization's active policy using available identity and contextual signals. These signals can include the authenticated user, device posture, location, requested application or resource, and relevant risk context. The resulting policy decision determines whether the specific request is permitted under current conditions.

Zscaler's Zero Trust Exchange applies policy at the point of access so users are connected only to authorized applications and resources, rather than being placed onto the network with broad standing access. This request-based enforcement supports continuous verification and limits access to what is explicitly allowed for the requested resource. It also enables policy to respond when relevant context changes, preserving least-privileged access throughout user activity. Zscaler describes this model in its Zero Trust Architecture overview and explains application-level access controls in its Zscaler Private Access documentation.

QUESTION NO: 8

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:

Legacy public-facing application architectures generally rely on a perimeter-based design because services are reachable and discoverable from the Internet. Establishing a DMZ that would include multiple products and services is therefore a standard approach: the DMZ creates a segmented zone in which externally accessible services can be isolated from more sensitive internal systems while security controls inspect and restrict inbound traffic. These deployments commonly require a large security stack including appliances that handle functions like global load balancing, firewalling, DDoS, and more. Each function addresses a different operational or security need at the public edge, such as traffic distribution, network-policy enforcement, and resilience against volumetric attacks.

A web application firewall (WAF) for protecting against DDoS and other botnet style attacks is also part of this layered model for web applications. A WAF applies application-aware inspection and policy enforcement to HTTP/S traffic, helping organizations identify and block malicious web requests, automated bot activity, and application-layer attack patterns. Together, these controls illustrate the traditional approach of placing multiple defensive technologies in front of publicly exposed services. Zscaler describes how zero trust instead seeks to reduce direct exposure by connecting authorized users to applications without placing those applications on the public Internet. See Zscaler's DMZ overview and Zscaler's WAF overview.

QUESTION NO: 9

An organization relies on a traditional remote-access VPN to connect users to its data-center network. Which two characteristics increase exposure compared with application-specific Zero Trust access? (Select 2)

A. Users are connected to a network from which multiple resources may be reachable.

B. A publicly reachable VPN gateway can become an attack target.

C. VPN encryption prevents all inspection and policy enforcement.

D. Remote users cannot authenticate before receiving access.

ANSWER: A B

Explanation:

A traditional VPN commonly provides a path into the private network, after which a connected endpoint may be able to reach multiple network resources according to network routing and segmentation. This broad network connectivity can increase opportunities for reconnaissance and lateral movement if the endpoint is compromised.

VPN gateways also commonly expose a publicly reachable entry point so remote users can establish the connection. In contrast, Zero Trust application access brokers authorized connections to specific applications without granting general network reachability. Encryption of the VPN tunnel protects traffic in transit, but it does not itself eliminate network-level exposure.