Zscaler

ZDTE

Zscaler Digital Transformation Engineer

For More Information – Visit link below:

https://www.examsempire.com/

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.

Latest Version: 9.0

Question: 1

In a typical authentication configuration, Zscaler fulfills which of the following roles?

A. SaaS gateway
B. Identity provider
C. Identity proxy
D. Service provider

Answer: D

Explanation:
In a typical enterprise authentication setup, Zscaler functions as the Service Provider (SP) within the SAML authentication framework. This aligns with Zscaler's architectural principle that identity verification is delegated to an external authoritative Identity Provider (IdP) such as Azure AD, Okta, Ping, or ADFS. Zscaler does not authenticate user credentials directly. Instead, it relies on the IdP to validate the user and then deliver a signed SAML assertion back to Zscaler.
When a user attempts to access the Zscaler service, the authentication request is redirected to the enterprise IdP. The IdP performs credential verification and returns a SAML assertion containing the authenticated user identity and associated attributes. Zscaler, acting as the SP, consumes and validates this assertion, then maps the identity to its internal user records or SCIM-synchronized directory objects. This identity becomes the basis for all ZIA/ZPA policy evaluation, including URL filtering, CASB controls, DLP policies, firewall rules, and access-control enforcement.
Since Zscaler depends on the IdP for primary identity verification and only consumes assertions, Zscaler's role is clearly defined as the Service Provider in a standard authentication configuration.

Question: 2

When using a Domain Joined posture element to allow access in a ZPA Access Policy, which statement is true?

A. Only some Linux operating systems have Domain Joined posture profile support in Zscaler.
B. When a ZPA Browser Access client attempts to access an application, Zscaler can determine if that device is joined to a particular domain.
C. If a 2nd domain and a sub-domain are needed in the Access Policy rule you must create a 2nd posture profile with the other domain and add it to the Access Policy.
D. Zscaler ZPA can contact the IDP such as Azure AD out-of-band to verify if a device is joined to a particular domain.

Answer: B

Explanation:
The Domain Joined posture element in ZPA evaluates whether a device belongs to a specific Active Directory domain. ZPA performs this evaluation using the device's local posture signals, either through the Zscaler Client Connector posture engine or through the browser-based posture evaluation framework used in ZPA Browser Access. When a user connects via Browser Access, ZPA can still determine domain membership by inspecting the allowed browser posture attributes provided by the endpoint, enabling device-based Zero Trust controls without requiring a full Client Connector installation.
Linux endpoints do not support domain-joined posture verification, making option A incorrect. Domain join validation is performed at the device level, not through the Identity Provider, because IdPs validate users, not device domain status, eliminating option D. ZPA's posture configuration allows you to define multiple domains within a single posture profile, so creating a second posture profile is unnecessary, making option C incorrect.
Therefore, the correct statement is that ZPA Browser Access can determine whether the device is joined to the specified domain, which aligns with the expected behavior of the domain-joined posture element.

Question: 3

Which connectivity service provides branches, on-premises data centers, and public clouds with fast and reliable internet access while enabling private applications with a direct-to-cloud architecture?

A. Zscaler Privileged Remote Access
B. Zscaler Browser Access
C. Zscaler App Connector
D. Zscaler Zero Trust SD-WAN

Answer: D

Explanation:
Zscaler Zero Trust SD-WAN is specifically designed to give branches, on-premises data centers, and workloads running in public clouds fast, reliable, and secure access to the internet and private applications using a direct-to-cloud architecture. In the Zscaler Digital Transformation Engineer curriculum, this service is positioned as the connectivity foundation that replaces legacy hub-andspoke MPLS and VPN designs with cloud-delivered Zero Trust connectivity.
Instead of backhauling traffic to central data centers, branches and sites establish lightweight, policydriven
tunnels directly to the Zscaler cloud, where security inspection and Zero Trust access decisions are applied. This architecture reduces latency, simplifies routing, and optimizes SaaS and internet performance while simultaneously enabling secure access to private applications without exposing them to the public internet.
App Connectors (option C) are used for application-side connectivity in ZPA, not for full branch or data center connectivity. Browser Access (option B) provides clientless application access for users, not network-level site connectivity. "Zscaler Privileged Remote Access" (option A) is not the term used for this broad connectivity service. Therefore, the only option that matches the described direct-to-cloud, multi-site connectivity role is Zscaler Zero Trust SD-WAN.

===========

Question: 4

What are the building blocks of App Protection?

A. Controls, Profiles, Policies
B. Policies, Controls, Profiles
C. Traffic Inspection, Vulnerability Identification, Action Based on User Behavior
D. Profiles, Controls, Policies

Answer: D

Explanation:
In Zscaler App Protection, the core design model is built around three fundamental building blocks presented in a specific logical order: Profiles, Controls, and Policies. The Digital Transformation Engineer material explains that App Protection's goal is to apply fine-grained security actions to applications and user sessions based on risk and context.
First, Profiles define who is being governed. They group users or devices that share common characteristics (such as department, location, or risk level). Next, Controls define what actions are allowed, restricted, or inspected. Examples include limiting copy-and-paste, file uploads and downloads, printing, clipboard usage, or enforcing additional inspection for sensitive content and risky behaviors. Finally, Policies define when and where those controls are applied by mapping profiles to specific applications or traffic categories under defined conditions (such as user risk posture, device posture, or access method).
Options A and B contain the same elements but in the wrong conceptual order compared to how App Protection is taught and implemented. Option C describes generic security concepts, not the explicit App Protection building-block terminology. Therefore, the correct sequence and terminology, matching the App Protection framework, is Profiles, Controls, Policies.
===========

Question: 5

A customer wants to set up an alert rule in ZDX to monitor the Wi-Fi signal on newly deployed laptops. What type of alert rule should they create?

A. Network
B. Device
C. Interface
D. Application

Answer: B

Explanation:

Zscaler Digital Experience (ZDX) organizes its telemetry and alerting around key domains: Application, Network, and Device. Wi-Fi signal strength is a client-side characteristic of the endpoint itself, measured from the user's device, not from the network path or the application service. In the ZDX training content, Wi-Fi signal, Wi-Fi link speed, CPU, memory, and similar metrics are clearly categorized under Device health.

When creating an alert rule to monitor newly deployed laptops, the administrator should therefore choose a Device-type alert and then select Wi-Fi signal–related metrics and thresholds. This allows ZDX to trigger alerts whenever the Wi-Fi signal on those endpoints falls below an acceptable level, helping operations teams quickly identify poor local wireless conditions that degrade user experience.

Network alerts are intended for end-to-end path health (latency, packet loss, DNS resolution, gateway reachability, etc.), and Application alerts focus on performance and availability of specific apps or services. "Interface" as a standalone alert type is not how ZDX structures its top-level alert categories; interface-related metrics are surfaced as device-side attributes. Consequently, the correct classification for Wi-Fi signal monitoring in ZDX is a Device alert rule.

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

Check our Customer Testimonials and ratings available on every product page.

Visit our website.

https://examsempire.com/