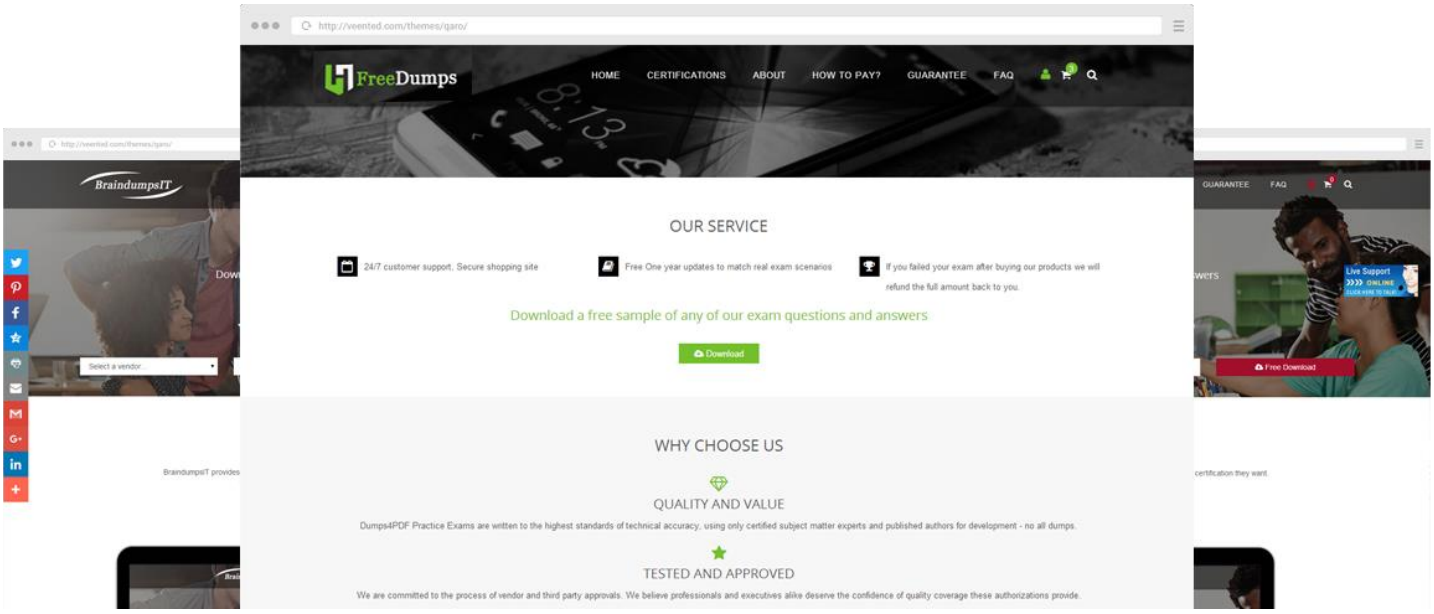
FreeDumps



WHAT PEOPLE SAY

Disclaimer Policy: The site does not guarantee the content of the comments. Because of the different time and the changes in the scope of the exam, it can produce different effect. Before you purchase the dump, please carefully read the product introduction from the page. In addition, please be advised the site will not be responsible for the content of the comments and contradictions between users.

> *Can not believe C2040-440! it is really same with the exam*

ATWOOD

> *If you want to pass exam casually I advise you to purchase study guide. A2010-578 study guide have a part of questions with real test.*

MILES

http://www.freedumps.top

Latest valid dumps torrent and free demo for certification exam prep

Exam : **ZDTE**

Title : Zscaler Digital Transformation Engineer

Vendor : Zscaler

Version : DEMO

NO.1 In the Zscaler Client Connector (ZCC) Admin Portal, which posture element is supported on Windows but not on macOS?

A. Client Certificate

B. Full Disk Encryption

C. Domain Joined

D. CrowdStrike ZTA Sensor Setting Score

Answer: D

Explanation:

Zscaler's Device Posture framework in Client Connector supports a broad set of posture checks on both Windows and macOS, such as Certificate Trust, Client Certificate, Firewall status, Full Disk Encryption, Domain Joined, and multiple EDR detections. These are listed in Zscaler technical training material as common capabilities for "Windows und macOS." However, Zscaler's advanced integration with CrowdStrike introduces additional posture signals based on Zero Trust Assessment (ZTA). In the same material, CrowdStrike ZTA Score is explicitly annotated with a Windows-specific minimum version ("CrowdStrike ZTA Score (Win v.3.4.0+)"), highlighting that this ZTA- based posture is implemented for Windows only in the current releases, while the shared list for macOS does not include its own ZTA-specific version.

The newer ZTE/EDU-202 engineer materials build on this by describing separate ZTA Device OS and Sensor scores, and the exam maps this Windows-only ZTA enforcement to the CrowdStrike ZTA Sensor Setting Score option. In contrast, Client Certificate, Full Disk Encryption, and Domain Joined are documented as cross-platform posture types, not restricted to Windows.

NO.2 What is the primary benefit of using a Custom Zscaler Connector for SaaS Application?

A. Minimum set of required credentials to access the SaaS Application Tenants

B. Temporary user credentials to access the SaaS Application Tenants

C. Broad access to all SaaS Application Tenants across Microsoft and Google

D. Full administrator credentials to access the SaaS Application Tenants

Answer: A

Explanation:

In Zscaler's SaaS Security and Data Protection services, a Custom Zscaler Connector (for example, for Google Workspace, Microsoft 365, or Salesforce) is designed so that Zscaler can connect to a specific SaaS tenant using only the minimum set of required credentials and scopes. The documentation for onboarding custom connectors explicitly emphasizes that, instead of providing full administrator rights, you authorize narrowly scoped API/OAuth permissions that allow Zscaler to scan data at rest and enforce security controls while adhering to least-privilege principles.

This minimal-credential approach reduces risk if the connector credentials are ever compromised, simplifies compliance audits, and aligns with modern security best practices. Zscaler needs just enough access to read, classify, and (where applicable) remediate or quarantine sensitive content in sanctioned SaaS applications, not broad tenant-wide admin access. Options suggesting temporary credentials, broad cross-tenant access, or full administrator rights contradict this design philosophy and the way the connectors are documented. Therefore, the primary benefit-and the key phrase you should associate with Custom Zscaler Connectors for the exam-is that they enable Zscaler to operate using a minimum set of required credentials for each SaaS Application tenant.

NO.3 What type of data would be protected by using Zscaler Indexed Document Matching (IDM)?

A. Excel sheets and other numerically based document types that usually contain proprietary financial calculations.
B. Sensitive data found in image files such as JPEGs and PNGs, or images embedded in documents like a Word file.
C. Specific, sensitive pieces of data such as customer credit card numbers and employee national identity numbers.
D. High-value documents that tend to carry sensitive data, such as medical forms and tax documents.
Answer: D
Explanation:
Zscaler Indexed Document Matching (IDM) is a DLP technique used to protect entire documents or large portions of text-based content, rather than discrete data fields. Administrators upload representative samples of "crown jewel" documents (for example, contract templates, medical forms, HR records, or tax documents).
Zscaler processes and indexes the textual content, then uses this index to detect when similar or identical document content is uploaded, shared, or exfiltrated through monitored channels.
This approach is ideal for high-value, unstructured documents that contain sensitive information in a repeatable format. It is distinct from Exact Data Match (EDM), which is used for structured field-level data such as credit card numbers or national IDs, and it is not optimized for pure image content or OCR-based detection. While IDM can apply to many file types (Word, PDF, spreadsheets that contain meaningful text, etc.), the core use case is protecting documents where overall content similarity matters.
Therefore, the best description is that IDM protects high-value documents that tend to carry sensitive data, such as medical forms and tax documents.

NO.4 A customer requires 2 Gbps of throughput through the GRE tunnels to Zscaler. Which is the ideal architecture?
A. Two primary and two backup GRE tunnels from internal routers with NAT enabled
B. Two primary and two backup GRE tunnels from border routers with NAT disabled
C. Two primary and two backup GRE tunnels from internal routers with NAT disabled
D. Two primary and two backup GRE tunnels from border routers with NAT enabled
Answer: B
Explanation:
Zscaler design guidance for GRE connectivity emphasizes three key principles: terminate GRE on border (edge) devices, avoid NAT on GRE source addresses, and scale bandwidth by using multiple tunnels. In Zscaler documentation and engineering training, each GRE tunnel is typically sized for up to about 1 Gbps of throughput. For a 2 Gbps requirement, customers are advised to deploy at least two primary GRE tunnels, with two additional backup tunnels for redundancy and failover.
These tunnels should terminate on border routers that own public IP addresses, ensuring optimal routing and simplifying troubleshooting. Zscaler specifically recommends that the public source IPs used for GRE must not be translated by NAT, because the Zscaler cloud must see the original, registered public IP to associate tunnels with the correct organization and enforce policy. Enabling NAT on GRE traffic can break tunnel establishment and lead to asymmetric or unpredictable routing. Using internal routers introduces extra hops and complexity and often requires NAT or policy-based routing, which goes against recommended best practices. Similarly, any architecture with NAT enabled on GRE traffic conflicts with Zscaler's published requirements. Therefore, the ideal and

recommended design for 2 Gbps via GRE is two primary and two backup GRE tunnels from border routers with NAT disabled.

NO.5 Which report provides valuable visibility and insight into end-user activity involving sensitive data on endpoints?

A. Malware report

B. Endpoint DLP report

C. Data usage report

D. Incidents report

Answer: B

Explanation:

In Zscaler, the Endpoint DLP report is specifically designed to give security teams visibility into how end users interact with sensitive data on their endpoints (laptops, desktops, etc.). This report aggregates activity such as copying, saving, printing, uploading, or otherwise handling sensitive content that is detected and classified by Zscaler Endpoint DLP. It focuses on data risk rather than just malware or traffic volumes, so it shows which files, users, and devices are involved in policy matches, along with the context of each event.

Unlike a generic malware or data usage report, the Endpoint DLP report is tightly aligned with DLP policies and data classifications you configure (such as PII, financial data, source code, or custom patterns). This allows you to quickly see which policies are triggering on endpoints, which channels or applications are most frequently involved, and where to fine-tune rules or add additional controls. Because it is endpoint-focused, it covers scenarios even when users are off the corporate network, giving a unified view across inline and endpoint DLP enforcement. For exam purposes, this is why Endpoint DLP report is the correct answer.

NO.6 What is the primary function of ZIA Public Service Edges in the Cloud Firewall architecture?

A. Managing endpoint security updates

B. Providing cloud storage services

C. Load balancing internet traffic

D. Acting as key policy enforcement engines

Answer: D

Explanation:

Within the ZIA Cloud Firewall and broader Zscaler Internet Access architecture, Public Service Edges (PSEs) are the core policy enforcement points. User traffic is steered (via tunnels, PAC files, or agents) to the nearest PSE, where Zscaler performs security inspection and policy evaluation. At this point, the Cloud Firewall, URL filtering, SSL inspection, IPS, sandboxing, and other security engines are applied according to the user's identity, group, location, and defined policies.

Although the PSEs naturally participate in traffic distribution across the global Zscaler cloud, their primary purpose is not generic load balancing or network transit; rather, they host the full security stack and make real- time allow/deny/log decisions. They also enforce bandwidth controls, application rules, and advanced threat protections before forwarding allowed traffic to the internet. They are not responsible for managing endpoint security updates or providing general cloud storage. Instead, they serve as inline security gateways that enforce Zero Trust access and granular firewall rules at scale.

Therefore, the correct description of their role in the Cloud Firewall architecture is that they act as

key policy enforcement engines.