Zscaler ZDTA Practice Questions

Shared by Haynes on 21-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What method does Zscaler Identity Threat Detection and Response use to gather information about AD domains?

Options:

A- Scanning network ports
B- Running LDAP queries
C- Analyzing firewall logs
D- Packet sniffing

Answer:

B

Explanation:

Identity Threat Detection and Response focuses on identity risk, particularly in directory environments such as Active Directory. To evaluate AD objects, relationships, permissions, and risky identity configurations, ITDR needs directory-level data rather than raw packet captures or firewall summaries. Option B (Running LDAP queries) is correct because LDAP queries are the standard mechanism for collecting structured AD domain information for identity-risk analysis.

Why the other options are incorrect:

A . Scanning network ports: Port scanning discovers open TCP/UDP services on hosts. ITDR needs AD identity data, so it queries the directory instead of scanning network sockets.

C . Analyzing firewall logs: Firewall logs show network sessions and policy outcomes. They do not expose AD object relationships, permissions, or identity hygiene the way LDAP directory queries do.

D . Packet sniffing: Packet sniffing captures traffic on the wire. ITDR is not passively sniffing packets here; it gathers structured domain information from Active Directory.

Question 2

Question Type: MultipleChoice

What happens after the Zscaler Client Connector receives a valid SAML response from the Identity Provider (IdP)?

Options:

A- The Zscaler Client Connector Portal authenticates the user directly.
B- There is no need for further actions as the SAML is valid, access is granted immediately.
C- The SAML response is sent back to the user's device for local validation.
D- Zscaler Internet Access validates the SAML response and returns an authentication token.

Answer:

D

Explanation:

After the Zscaler Client Connector (ZCC) receives a valid SAML response, Zscaler Internet Access (ZIA) takes over to validate the SAML assertion. Upon successful validation, ZIA issues an authentication token that allows the user to access services securely. This centralized validation ensures authentication integrity and enables seamless policy enforcement across Zscaler services.

Question 3

Question Type: MultipleChoice

What is the preferred method for authentication to access oneAPI?

Options:

A- OpenID Connect (OIDC)
B- Transport Layer Security (TLS)
C- Security Assertion Markup Language (SAML)
D- System for Cross-domain Identity Management (SCIM)

Answer:

A

Explanation:

The preferred method for authentication to access Zscaler's oneAPI is OpenID Connect (OIDC). OIDC is an identity layer on top of the OAuth 2.0 protocol and provides a modern, secure, and scalable way to authenticate users and services interacting with the API.

The study guide notes that OIDC supports flexible and secure authentication, making it the recommended choice for API access management within Zscaler's platform.

Question 4

Question Type: MultipleChoice

Which of the following is a valid action for a SaaS Security API Data Loss Prevention Rule?

Options:

A- Enable AI/ML based Smart Browser Isolation
B- Quarantine Mai ware
C- Create Zero Trust Network Decoy
D- Remove External Collaborators and Sharable Link

Answer:

D

Explanation:

In SaaS Security API DLP policies you can choose ''Remove External Collaborators and Shareable Link'' as the enforcement action - Zscaler will report the incident, revoke any external collaborators on the file, and delete its external share links.

Question 5

Question Type: MultipleChoice

When configuring Applications to be monitored, what probe types can be created?

Options:

A- Page Fetch Time Probe and Cloud Path Probe
B- Web Probe and Page Fetch Time Probe
C- Page Fetch Time Probe and Server Response time Probe
D- Web Probe and Cloud Path Probe

Answer:

D

Explanation:

When you set up application monitoring in ZDX, you can create Web Probes to measure application performance from the browser and Cloud Path Probes to map and monitor the network path to those applications.

Question 6

Question Type: MultipleChoice

A user has opened a support case to complain about poor user experience when trying to manage their AWS resources. How could a helpdesk administrator get a useful root cause analysis to help isolate the issue in the least amount of time?

Options:

A- Check the Zscaler Trust page for any indications of cloud outages or incidents that would be causing a slowdown.
B- Check the user's ZDX score for a period of low score for AWS and use Analyze Score to get the ZDX Y-Engine analysis.
C- Do a Deep Trace on the user's traffic and check for excessive DNS resolution times and other slowdowns.
D- Initiate a packet capture from Zscaler Client Connector and escalate the case to have the trace analyzed for root cause.

Answer:

D

Explanation:

By reviewing the user's ZDX score for AWS and running ''Analyze Score,'' the Y Engine automatically correlates metrics (network, client, and application) to pinpoint the root cause, delivering targeted insights far faster than manual tracing or external outage checks.

Question 7

Question Type: MultipleChoice

Assume that you have four data centers around the globe, each hosting multiple applications for your users. What is the minimum number of App Connectors you should deploy?

Assume that you have four data centers around the globe, each hosting multiple applications for your users. What is the minimum number of App Connectors you should deploy?

Options:

A- Six - one per data center plus two for cold standby.
B- Eight -two per data center.
C- Four - one per data center.
D- Sixteen - to support a full mesh to the other data centers.

Answer:

B

Explanation:

You need at least two App Connectors per data center to ensure high availability and load distribution, so with four data centers the minimum total is eight.

Question 8

Question Type: MultipleChoice

What is the recommended minimum number of App connectors needed to ensure resiliency?

Options:

A- 2
B- 6
C- 4
D- 3

Answer:

A

Explanation:

The recommended minimum number of App connectors to ensure resiliency in Zscaler Private Access is 2. Having at least two App connectors provides redundancy, so if one connector fails or is unavailable, the other can continue to provide access without interruption. This recommendation is critical to maintaining high availability and fault tolerance for internal application access.

The study guide specifies this minimum to ensure continuity and reliability of application access through ZPA.

Question 9

Question Type: MultipleChoice

What is one of the four steps of a cyber attack?

Options:

A- Find Cash Safe
B- Find Email Addresses
C- Find Least Secure Office Building
D- Find Attack Surface

Answer:

D

Explanation:

One of the four essential steps of a cyber attack is to find the attack surface. This step involves identifying vulnerabilities, entry points, and targets within an organization's network or systems that can be exploited by attackers.

The study guide outlines this as a critical phase in the cyber kill chain, where attackers map out potential avenues for compromise.

Question 10

Question Type: MultipleChoice

Which option best is a feature of ITDR (Identity Threat Detection and Response)?

Options:

A- Prevents Patient Zero Infections
B- Reduces identity related risks
C- Prevents connections to Embargoed Countries
D- Blocks malicious traffic by dropping packets

Answer:

B

Explanation:

Identity Threat Detection and Response (ITDR) solutions are specifically designed to identify and remediate identity centric risks - continuously assessing user and service identities to detect compromised credentials, misconfigurations, or risky behaviors, thereby reducing overall identity related risk.

Question 11

Question Type: MultipleChoice

Which option best are correct request methods when configuring a URL filtering rule with a Caution action?

Options:

A- Connect, Get, Head
B- Options, Delete, Put
C- Get, Delete, Trace
D- Connect, Post, Put

Answer:

A

Explanation:

When you configure a URL Filtering rule with the Caution action, the only HTTP methods you can select for that rule are CONNECT, GET, and HEAD.

Question 12

Question Type: MultipleChoice

What does Zscaler Advanced Firewall support that Zscaler Standard Firewall does not?

Options:

A- Destination NAT
B- FQDN Filtering with wildcard
C- DNS Dashboards, Insights and Logs
D- DNS Tunnel and DNS Application Control

Answer:

D

Explanation:

Zscaler Advanced Firewall supports DNS Tunnel and DNS Application Control, capabilities that

are not available in the Standard Firewall. This enhances detection and control of DNS-based threats and allows granular enforcement over DNS queries and responses to prevent data exfiltration and command and control activities.

Question 13

Question Type: MultipleChoice

Which Zscaler feature detects whether an intruder is accessing your internal resources?

Options:

A- SandBox
B- SSL Decryption Bypass
C- Browser Isolation
D- Deception

Answer:

D

Explanation:

The Deception feature in Zscaler detects intruders attempting to access internal resources by deploying deceptive assets or traps that identify unauthorized or suspicious activity. This proactive approach to threat detection helps identify attackers who have bypassed other defenses.

To Get Premium Files for ZDTA Visit

https://www.p2pexams.com/products/zdta

For More Free Questions Visit

https://www.p2pexams.com/zscaler/pdf/zdta

