

Zscaler

Exam Questions ZDTA

Zscaler Digital Transformation Administrator



NEW QUESTION 1

What conditions can be referenced for Trusted Network Detection?

- A. Hostname Resolution, Network Adapter IP, Default Gateway
- B. DNS Servers, DNS Search Domain, Network Adapter IP
- C. Hostname Resolution, DNS Servers, Geo Location
- D. DNS Search Domain, DNS Server, Hostname Resolution

Answer: D

NEW QUESTION 2

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

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

Answer: B

NEW QUESTION 3

In support of data privacy about TLS/SSL inspection, when you subscribe to ZIA, you enter into what kind of agreement?

- A. Zscaler Compliance Policy
- B. Zscaler Privacy Policy
- C. Acceptable Use Policy
- D. Zscaler Data Processing Agreement

Answer: D

NEW QUESTION 4

An administrator wants to allow users to access a wide variety of untrusted URLs. Which of the following would allow users to access these URLs in a safe manner?

- A. Browser Isolation
- B. App Connector
- C. Zscaler Private Access
- D. Zscaler Client Connector

Answer: A

NEW QUESTION 5

The security exceptions allow list for Advanced Threat Protection apply to which of the following Policies?

- A. Sandbox
- B. URL Filtering
- C. File Type Control
- D. IPS Control

Answer: A

NEW QUESTION 6

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

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

Answer: D

NEW QUESTION 7

What transport mechanism will Zscaler Client Connector use to forward traffic to the Zero Trust Exchange when configured for Tunnel 2.0?

- A. Zscaler Client Connector will encapsulate the user's traffic in GRE tunnels to the ZTE.
- B. Zscaler Client Connector will encapsulate the user's traffic in IPsec tunnels to the ZTE.
- C. Zscaler Client Connector will encapsulate the user's traffic in dTLS/TLS tunnels to the ZTE.
- D. Zscaler Client Connector will encapsulate the user's traffic in HTTP Connect tunnels to the ZTE.

Answer: C

NEW QUESTION 8

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?

- 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

NEW QUESTION 9

What is the purpose of a Microtunnel (M-Tunnel) in Zscaler?

- A. To provide an end-to-end communication channel between ZCC clients
- B. To provide an end-to-end communication channel to Microsoft Applications such as M365
- C. To create an end-to-end communication channel to Azure AD for authentication
- D. To create an end-to-end communication channel to internal applications

Answer: D

NEW QUESTION 10

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?

- 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

NEW QUESTION 10

According to the Zero Trust Exchange Functional Services Diagram, which services does Antivirus belong to?

- A. Platform Services
- B. Access Control Services
- C. Security Services
- D. Advanced Threat Prevention Services

Answer: C

NEW QUESTION 13

What is the immediate outcome or effect when the Zscaler Office 365 One Click Rule is enabled?

- A. All traffic undergoes mandatory SSL inspection.
- B. Office 365 traffic is exempted from SSL inspection and other web policies.
- C. Non-Office 365 traffic is blocked.
- D. All Office 365 drive traffic is blocked.

Answer: B

NEW QUESTION 16

What does the user risk score enable a user to do?

- A. Compare the user risk score with other companies to evaluate users vs other companies.
- B. Determine whether or not a user is authorized to view unencrypted data.
- C. Configure stronger user-specific policies to monitor & control user-level risk exposure.
- D. Determine if a user has been compromised

Answer: C

NEW QUESTION 17

When the Zscaler Client Connector launches, which portal does it initially interact with to understand the user's domain and identity provider (IdP)?

- A. Zscaler Private Access (ZPA) Portal
- B. Zscaler Central Authority
- C. Zscaler Internet Access (ZIA) Portal
- D. Zscaler Client Connector Portal

Answer: B

NEW QUESTION 20

For a deployment using both ZIA and ZPA set of services, what is the best authentication solution?

- A. Use forms Authentication in ZPA and SAML in ZIA
- B. Use forms Authentication in ZIA and SAML in ZPA
- C. Configure Authentication using SAML on both ZIA and ZPA
- D. Use forms Authentication for both ZIA and ZPA

Answer: C

NEW QUESTION 24

How is data gathered with ZDX Advanced client performance?

- A. By generating synthetic transactions to designated Internet and Private applications every 5 minutes and measuring the performance of those sessions.
- B. By constantly analyzing live user sessions to both Internet and Private applications and measuring the performance of those sessions.
- C. By using AI predictive analysis ZDX can extrapolate near-term client performance based upon recent past data observed.
- D. By constantly analyzing live user sessions to critical SaaS applications and measuring the performance of those sessions.

Answer: B

NEW QUESTION 25

If you're migrating from an on-premises proxy, you will already have a proxy setting configured within the browser or within the system. With Tunnel Mode, the best practice is to configure what type of proxy configuration?

- A. Execute a GPO update to retrieve the proxy settings from AD.
- B. Enforce no Proxy Configuration.
- C. Use Web Proxy Auto Discovery (WPAD) to auto-configure the proxy.
- D. Use an automatic configuration script (forwarding PAC file).

Answer: B

NEW QUESTION 30

When a SAML IDP returns an assertion containing device attributes, which Zscaler component consumes the attributes first, for policy creation?

- A. Enforcement node
- B. Zscaler SAML SP
- C. Mobile Admin Portal
- D. Zero Trust Exchange

Answer: D

NEW QUESTION 35

What Malware Protection setting can be selected when setting up a Malware Policy?

- A. Isolate
- B. Bypass
- C. Block
- D. Do Not Decrypt

Answer: C

NEW QUESTION 36

Which of the following are correct request methods when configuring a URL filtering rule with a Caution action?

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

Answer: A

NEW QUESTION 37

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

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

Answer: D

NEW QUESTION 39

What can Zscaler Client Connector evaluate that provides the most thorough determination of the trust level of a device as criteria for an access policy enabling remote access to sensitive private applications?

- A. Client Type
- B. SCIM User Attributes
- C. Trusted Network

D. Posture Profiles

Answer: D

NEW QUESTION 43

Which proprietary technology does Zscaler use to calculate risk attributes dynamically for websites?

- A. Third-Party Sandbox
- B. Zscaler PageRisk
- C. Browser Isolation Feedback Form
- D. Deception Controller

Answer: B

NEW QUESTION 45

Within ZPA, the mapping relationship between Connector Groups and Server Groups can best be defined as which of the following?

- A. Server Groups are configured for Dynamic Server Discovery so that mapped Connector Groups can then DNS resolve individual application Segment Groups.
- B. Connector Groups are configured for Dynamic Server Discovery so that mapped Server Groups can DNS resolve and advertise the applications.
- C. Connector Groups are configured for Dynamic Server Discovery so that ZPA can steer traffic through the appropriate Server Group.
- D. Server Groups are configured for Dynamic Server Discovery so that mapped Connector Groups can DNS resolve and make health checks toward the application.

Answer: D

NEW QUESTION 49

Which attack type is characterized by a commonly used website or service that has malicious content like malicious JavaScript running on it?

- A. Watering Hole Attack
- B. Pre-existing Compromise
- C. Phishing Attack
- D. Exploit Kits

Answer: A

NEW QUESTION 50

When configuring Zscaler Private Access, what is the function of the Server Group?

- A. Maps FQDNs to IP Addresses
- B. Maps Applications to FQDNs
- C. Maps App Connector Groups to Application Segments
- D. Maps Applications to Application Groups

Answer: A

NEW QUESTION 53

Which Platform Service enables visibility into the headers and payload of encrypted transactions?

- A. Policy Framework
- B. TLS Decryption
- C. Reporting and Logging
- D. Device Posture

Answer: B

NEW QUESTION 58

How does a Zscaler administrator troubleshoot a certificate pinned application?

- A. They could look at SSL logs for a failed client handshake.
- B. They could reboot the endpoint device.
- C. They could inspect the ZIA Web Policy.
- D. They could look into the SaaS application analytics tab.

Answer: A

NEW QUESTION 61

Which type of attack plants malware on commonly accessed services?

- A. Remote access trojans
- B. Phishing
- C. Exploit kits
- D. Watering hole attack

Answer: D

NEW QUESTION 65

What is the main purpose of Sandbox functionality?

- A. Block malware that we have previously identified
- B. Build a test environment where we can evaluate the result of policies
- C. Identify Zero-Day Threats
- D. Balance threat detection across customers around the world

Answer: C

NEW QUESTION 70

SSH use or tunneling was detected and blocked by which feature?

- A. Cloud App Control
- B. URL Filtering
- C. Advanced Threat Protection
- D. Mobile Malware Protection

Answer: A

NEW QUESTION 74

Which of the following options will protect against Botnet activity using IPS and Yara type content analysis?

- A. Command and Control Traffic
- B. Ransomware
- C. Trojans
- D. Adware/Spyware Protection

Answer: A

NEW QUESTION 79

Can Notifications, based on Alert Rules, be sent with methods other than email?

- A. Email is the only method for notifications as that is universally applicable and no other way of sending them makes sense.
- B. In addition to email, text messages can be sent directly to one cell phone to alert the CISO who is then coordinating the work on the incident.
- C. Leading ITSM systems can be connected to the Zero Trust Exchange using a NSS server, which will then connect to ITSM tools and forwards the alert.
- D. In addition to email, notifications, based on Alert Rules, can be shared with leading ITSM or UCAAS tools over Webhooks.

Answer: B

NEW QUESTION 81

Which of the following is the preferred method for authentication in a OneAPI environment?

- A. OIDC
- B. SCIM
- C. SAML
- D. EntraID

Answer: A

NEW QUESTION 82

What is the primary function of the on-premises VM in the EDM process?

- A. To local analyze cloud transactions for potential PII exfiltration.
- B. To replicate sensitive data across all organizational servers.
- C. To automate the indexing process by creating hashes for structured data elements.
- D. To store sensitive data securely and prevent unauthorized data access.

Answer: A

NEW QUESTION 83

What is the purpose of the Zscaler Client Connector providing the authentication token to the Zscaler Client Connector Portal after it is received from Zscaler Internet Access?

- A. To bypass multifactor authentication (MFA) during the enrollment process
- B. To immediately grant the user access to Zscaler Private Access resources
- C. To enable the portal to register the user's device and pass the registration to Zscaler Internet Access
- D. To share the authentication token with the SAML IdP to validate the user session

Answer: C

NEW QUESTION 87

Does the Access Control suite include features that prevent lateral movement?

- A. N
- B. Access Control Services will only control access to the Internet and cloud applications.

- C. Ye
- D. Controls for segmentation and conditional access are part of the Access Control Services.
- E. Ye
- F. The Cloud Firewall will detect network segments and provide conditional access.
- G. N
- H. The endpoint firewall will detect network segments and steer access.

Answer: B

NEW QUESTION 91

Does the Cloud Firewall detect evasion techniques that would allow applications to communicate over non-standard ports to bypass its controls?

- A. The Cloud Firewall includes Deep Packet Inspection, which detects protocol evasions and sends the traffic to the respective engines for inspection and handling.
- B. Zscaler Client Connector will prevent evasion on the endpoint in conjunction with the endpoint operating system's firewall.
- C. As traffic usually is forwarded from an on-premise firewall, this firewall will handle any evasion and will make sure that the protocols are corrected.
- D. The Cloud Firewall includes an IPS engine, which will detect the evasion techniques and will just block the transactions as it is invalid.

Answer: A

NEW QUESTION 96

Which of the following is a common use case for adopting Zscaler's Data Protection?

- A. Reduce your Internet Attack Surface
- B. Prevent download of Malicious Files
- C. Prevent loss to Internet and Cloud Apps
- D. Securely connect users to Private Applications

Answer: C

NEW QUESTION 98

What is Zscaler's rotation policy for intermediate certificate authority certificates?

- A. Certificates are rotated every 90 days and have a 180-day expiration.
- B. Lifetime certificates have no expiration date.
- C. Certificates are rotated every seven days and have a 14-day expiration.
- D. Certificates are issued dynamically and expire in 24 hours.

Answer: C

NEW QUESTION 100

While troubleshooting a user's slow application access, can a ZDX administrator see degradations in Wi-Fi signal strength?

- A. Yes, the Wi-Fi hop latency is shown on a cloud path probe.
- B. Ye
- C. but the current Wi-Fi signal strength is only displayed when doing a deep trace.
- D. No, ZDX only works on hardwired devices.
- E. Yes, a low Wi-Fi signal may be seen in either the results of a Cloud Path Probe or in the device health Wi-Fi signal indicator.

Answer: D

NEW QUESTION 103

What is one business risk introduced by the use of legacy firewalls?

- A. Performance issues
- B. Reduced management
- C. Low costs
- D. Low licensing support

Answer: A

NEW QUESTION 107

When users are authenticated using SAML, what are the two most efficient ways of provisioning the users?

- A. Hosted User Database and Directory Server Synchronization
- B. SAML and Hosted User Database
- C. SCIM and Directory Server Synchronization
- D. SCIM and SAML Autoprovisioning

Answer: D

NEW QUESTION 111

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

- A. 2

- B. 6
- C. 4
- D. 3

Answer: A

NEW QUESTION 112

Which of the following are types of device posture?

- A. Detect CrowdStrike, CrowdStrike ZTA score, First name
- B. Certificate Trust, File Path, Full Disk Encryption
- C. Domain Joined, Process Check, Deception Check
- D. Unauthorized Modification, OS Version, License Key

Answer: B

NEW QUESTION 114

Which of the following components is installed on an endpoint to connect users to the Zero Trust Exchange regardless of their location - home, work, while traveling, etc.?

- A. Client connector
- B. Private Service Edge
- C. IPSec/GRE Tunnel
- D. App Connector

Answer: A

NEW QUESTION 117

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

ZDTA Practice Exam Features:

- * ZDTA Questions and Answers Updated Frequently
- * ZDTA Practice Questions Verified by Expert Senior Certified Staff
- * ZDTA Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * ZDTA Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The ZDTA Practice Test Here](#)