



Zscaler

Exam Questions ZDTA

Zscaler Digital Transformation Administrator

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

Which types of Botnet Protection are supplied by Advanced Threat Protection?

- A. Malicious file downloads, Command traffic (sending / receiving), Data exfiltration
- B. Connections to known C&C servers, Command traffic (sending / receiving), Unknown C&C using AI/ML
- C. Connections to known C&C servers, Detection of phishing sites, Access to spam sites
- D. Vulnerabilities in web server applications, Unknown C&C using AI/ML, Vulnerable ActiveX controls

Answer: B

NEW QUESTION 2

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS includes which of the following?

- A. Spyware Callback
- B. Anonymizers
- C. Cookie Stealing
- D. IRC Tunneling

Answer: C

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

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 6

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 7

How is the relationship between App Connector Groups and Server Groups created?

- A. The relationship between App_ Connector Groups and Server Groups is established dynamically in the Zero Trust Exchange as users try to access Applications
- B. When a new Server Group is created it points to the App_ Connector Groups that provide visibility to this Server Group
- C. Both App Connector Groups and Server Groups are linked together via the Data Center element
- D. When you create a new App Connector Group you must select the list of Server Groups to which it provides visibility

Answer: B

NEW QUESTION 8

Zscaler forwards the server SSL/TLS certificate directly to the user's browser session in which situation?

- A. When traffic contains a known threat signature.
- B. When web traffic is on custom TCP ports.
- C. When traffic is exempted in SSL Inspection policy rules.
- D. When user has connected to server in the past.

Answer: C

NEW QUESTION 9

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 10

Fundamental capabilities needed by other services within the Zscaler Zero Trust Exchange are provided by which of these?

- A. Access Control Services
- B. Digital Experience Monitoring
- C. Cyber Security Services
- D. Platform Services

Answer: D

NEW QUESTION 10

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

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

Answer: D

NEW QUESTION 12

You've configured the API connection to automatically download Microsoft Information Protection (MIP) labels into ZIA; where will you use these imported labels to protect sensitive data in motion?

- A. Creating a custom DLP Dictionary
- B. Creating a SaaS Security Posture Control Policy.
- C. Creating a File Type Control Policy.
- D. Creating a custom DLP Policy.

Answer: D

NEW QUESTION 15

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 17

What is the default policy configuration setting for checking for Viruses?

- A. Allow
- B. Block
- C. Unwanted Applications
- D. Malware Protection

Answer: B

NEW QUESTION 20

Zscaler Platform Services works upon unencrypted data from encrypted communications due to which of the following?

- A. Antivirus
- B. Tenant Restrictions
- C. Web Filtering
- D. TLS Inspection

Answer: D

NEW QUESTION 25

The Forwarding Profile defines which of the following?

- A. Fallback methods and behavior when a DTLS tunnel cannot be established
- B. Application PAC file location
- C. System PAC file when off trusted network
- D. Fallback methods and behavior when a TLS tunnel cannot be established

Answer: A

NEW QUESTION 28

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 33

Which of the following scenarios would generate a ??Patient 0?? alert?

- A. Zscaler's AI/ML based Smart Browser Isolation was triggered due to a users accessing a newly-registered domain.
- B. A new malicious file was detected by the sandbox due to an ??allow and scan?? First-Time Action in the sandbox policy.
- C. A new malicious file was detected by the sandbox due to an ??quarantine?? First-Time Action in the sandbox policy.
- D. Zscaler detected a HIPAA violation with in-band Data Protection scanning.

Answer: B

NEW QUESTION 37

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 40

What are common delivery mechanisms for malware?

- A. Malware downloads from web pages
- B. Personal emails, company documents, OneDrive
- C. Spam, exploit kits, USB drives, video streaming
- D. Phishing, Exploit Kits, Watering Holes, Pre-existing Compromise

Answer: D

NEW QUESTION 44

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 46

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 49

Layered defense throughout an organization security platform is valuable because of which of the following?

- A. Layered defense increases costs to attackers to operate.
- B. Layered defense from multiple vendor solutions easily share attacker data.
- C. Layered defense ensures attackers are prevented eventually.
- D. Layered defense with multiple endpoint agents protects from attackers.

Answer: A

NEW QUESTION 52

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

- 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

NEW QUESTION 56

Which type of malware is specifically used to deliver other malware?

- A. RAT
- B. Maldocs
- C. Downloaders
- D. Exploitation tool

Answer: C

NEW QUESTION 58

The Zscaler platform can protect against malicious files, URLs and content based on a number of criteria including reputation type. What type of checking is virus scanning?

- A. Malware protection
- B. File reputation
- C. SHA-256 hashing
- D. Site reputation

Answer: A

NEW QUESTION 63

Which Advanced Threats policy can be configured to protect users against a credential attack?

- A. Configure Advanced Cloud Sandbox policies.
- B. Block Suspected phishing sites.
- C. Enable Watering Hole detection.
- D. Block Windows executable files from uncategorized websites.

Answer: B

NEW QUESTION 66

Zscaler Data Protection supports custom dictionaries.

What actions can administrators take with these dictionaries to protect data in motion?

- A. Define specific keywords, phrases, or patterns relevant to their organization's sensitive data policy.
- B. Define specific governance and regulations relevant to their organization's sensitive data policy.
- C. Define specific SaaS tenant relevant to their organization's sensitive data policy
- D. Define specific file types relevant to their organization's sensitive data policy.

Answer: A

NEW QUESTION 69

As technology that exists for a very long period of time, has URL Filtering lost its effectiveness?

- A. URL Filter is the most commonly used web filtering technique in the arsena
- B. It acts as first line of defense.
- C. In a modern cloud world, access to all Internet sites and cloud applications should be granted by default
- D. URL Filtering is no longer needed.
- E. URL Filtering has been replaced by CASB functionality through blocking access to all Internet sites and only allowing a few corporate applications.
- F. URL Filtering is outdated and no longer needed

G. The rise of HTTPS leads renders URL Filtering ineffective as all traffic is encrypted.

Answer: A

NEW QUESTION 71

What is a ZIA Sublocation?

- A. The section of a corporate Location used to separate traffic, like traffic from employees from guest traffic
- B. The section of a corporate Location that sends traffic to a Subcloud
- C. Every one of the sections in a Corporate Location that use overlapping IP addresses
- D. A way to separate generic traffic from that coming from Client Connector

Answer: A

NEW QUESTION 75

Which of the following is unrelated to the properties of 'Trusted Networks'?

- A. DNS Server
- B. Default Gateway
- C. Org ID
- D. Network Range

Answer: C

NEW QUESTION 79

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 82

What is the scale used to represent a users Zscaler Digital Experience (ZDX) score?

- A. 1-100
- B. 1-10
- C. 1 - 1000
- D. 0 - 50

Answer: A

NEW QUESTION 85

Which of the following is a unified management console for internet and SaaS applications, private applications, digital experience monitoring and endpoint agents?

- A. identity Admin Portal
- B. Mobile Admin Portal
- C. Experience Center
- D. One API

Answer: C

NEW QUESTION 89

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 92

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 96

Can URL Filtering make use of Cloud Browser Isolation?

- A. N
- B. Cloud Browser Isolation is a separate platform.
- C. N
- D. Cloud Browser Isolation is only a feature of Advanced Threat Defense.
- E. Ye
- F. After blocking access to a site, the user can manually switch on isolation.
- G. Ye
- H. Isolate is a possible Action for URL Filtering.

Answer: D

NEW QUESTION 98

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 102

What does TLS Inspection for Zscaler Internet Access secure public internet browsing with?

- A. Storing connection streams for future customer review.
- B. Removing certificates and reconnecting client connection using HTTP.
- C. Intermediate certificates are created for each client connection.
- D. Logging which clients receive the original webserver certificate.

Answer: C

NEW QUESTION 106

.....

Relate Links

100% Pass Your ZDTA Exam with Examible Prep Materials

<https://www.examible.com/ZDTA-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.examible.com/>