



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

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

When filtering user access to certain web destinations what can be a better option, URL or Cloud Application filtering Policies?

- A. Cloud Application policies provide better access control.
- B. URL filtering policies provide better access control.
- C. Wherever possible URL policies are recommended.
- D. Both provide the same filtering capabilities.

Answer: A

NEW QUESTION 5

Zscaler Client Connector checks for software updates automatically at which interval?

- A. Every 6 hours
- B. Every 12 hours
- C. Every 2 hours
- D. Every 24 hours

Answer: C

NEW QUESTION 6

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 7

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 8

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 9

What does Advanced Threat Protection defend users from?

- A. Vulnerable JavaScripts
- B. Large iFrames
- C. Malicious active content
- D. Command injection attacks

Answer: C

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 10

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 14

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 15

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 19

What mechanism identifies the ZIA Service Edge node that the Zscaler Client Connector should connect to?

- A. The IP ranges included/excluded in the App Profile
- B. The PAC file used in the Forwarding Profile
- C. The PAC file used in the Application Profile
- D. The Machine Key used in the Application Profile

Answer: B

NEW QUESTION 22

From a user perspective, Zscaler Bandwidth Control performs traffic shaping and buffering on what direction(s) of traffic?

- A. Outbound traffic is shape
- B. Inbound or localhost traffic is unshaped.

- C. Outbound or inbound traffic is shape
- D. Localhost traffic is unshaped.
- E. Inbound traffic is shape
- F. Outbound or localhost traffic is unshaped.
- G. Localhost traffic is shape
- H. Outbound or Inbound traffic is unshaped.

Answer: A

NEW QUESTION 27

How would an administrator retrieve the access token to use the Zscaler One API?

- A. The administrator needs to send a POST request along with the required parameters to ZIdentity's token endpoint.
- B. The administrator needs to send a GET request along with the required parameters to ZIdentity's token endpoint.
- C. The administrator needs to logon to the ZIA portal to generate the access token with Super Admin role.
- D. The administrator needs to logon to the ZIA portal to generate the access token with API Admin role.

Answer: A

NEW QUESTION 31

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 32

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

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

Answer: D

NEW QUESTION 35

What is the ZIA feature that ensures certain SaaS applications cannot be accessed from an unmanaged device?

- A. Tenant Restriction
- B. Identity Proxy
- C. Out-of-band Application Access
- D. SaaS Application Access

Answer: A

NEW QUESTION 37

Zscaler Advanced Threat Protection (ATP) is a key capability within Zscaler Internet Access (ZIA), protecting users against attacks such as phishing. Which of the following is NOT part of the ATP workflow?

- A. IPS coverages for client-side and server-side
- B. Reporting high latency from the CEO's Teams call due to a low WiFi signal
- C. Comprehensive URL categories for newly registered domains
- D. Preventing the download of a password protected zip file

Answer: B

NEW QUESTION 42

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 44

Which of the following is a feature of ITDR (Identity Threat Detection and Response)?

- 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

NEW QUESTION 49

Which of the following is an unsupported tunnel type?

- A. Generic Routing and Encapsulation (GRE)
- B. HTTP Connect Tunnels
- C. Proprietary Microtunnels
- D. Secure Socket Tunneling Protocol (SSTP)

Answer: D

NEW QUESTION 50

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 55

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 57

Which feature does Zscaler Client Connector Z-Tunnel 2.0 enable over Z-Tunnel 1.0?

- A. Enables SSL Inspection for Client Connector
- B. Inspection of all ports and protocols via Cloud Firewall
- C. Enables Browser Isolation
- D. Enables multicast traffic

Answer: B

NEW QUESTION 59

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 64

Which filtering policy blocked access to the Network Application?

- A. Sandbox
- B. Browser Control
- C. Firewall Filtering
- D. DLP

Answer: C

NEW QUESTION 65

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 67

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

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

Answer: C

NEW QUESTION 71

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 74

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 77

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 81

Is SCIM required for ZIA?

- A. Depends
- B. Maybe
- C. No
- D. Yes

Answer: C

NEW QUESTION 85

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 88

Which of the following DLP Notification methods can be used to forward a copy of the data that triggered the DLP policy to the auditor?

- A. Email Notification Template
- B. NSS Log Forwarding to SIEM
- C. SMS Text Message via PagerDuty
- D. Zscaler Client Connector pop-up message

Answer: A

NEW QUESTION 93

Which SaaS platform is supported by Zscaler's SaaS Security Posture Management (SSPM)?

- A. Amazon S3

- B. Webex Teams
- C. Dropbox
- D. Google Workspace

Answer: C

NEW QUESTION 95

Which Advanced Threat Protection feature restricts website access by geographic location?

- A. Spyware Callback
- B. Botnet Protection
- C. Blocked Countries
- D. Browser Exploits

Answer: C

NEW QUESTION 96

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 98

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 100

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 101

When configuring an inline Data Loss Prevention policy with content inspection, which of the following are used to detect data, allow or block transactions, and notify your organization's auditor when a user's transaction triggers a DLP rule?

- A. Hosted PAC Files
- B. Index Tool
- C. DLP engines
- D. VPN Credentials

Answer: C

NEW QUESTION 105

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 108

Which is an example of Inline Data Protection?

- A. Preventing the copying of a sensitive document to a USB drive.
- B. Preventing the sharing of a sensitive document in OneDrive.
- C. Analyzing a customer's M365 tenant for security best practices.
- D. Blocking the attachment of a sensitive document in webmail.

Answer: D

NEW QUESTION 109

What is the preferred method for authentication to access oneAPI?

- 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

NEW QUESTION 113

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 116

Which list of protocols is supported by Zscaler for Privileged Remote Access?

- A. RDP, VNC and SSH
- B. RDP, SSH and DHCP
- C. SSH, DNS and DHCP
- D. RDP, DNS and VNC

Answer: A

NEW QUESTION 119

Which of the following methods can be used to notify an end-user of a potential DLP violation in Zscaler's Workflow Automation solution?

- A. Notifications in MS Teams / Slack
- B. SMS text message.
- C. Automated phone call.
- D. Twitter post with custom hashtan

Answer: A

NEW QUESTION 123

.....

Relate Links

100% Pass Your ZDTA Exam with ExamBible Prep Materials

<https://www.exambible.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.exambible.com/>