Exam Questions ZDTA

Zscaler Digital Transformation Administrator

https://www.2passeasy.com/dumps/ZDTA/

NEW QUESTION 1
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 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
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 4
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 5
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 6
Which Risk360 key focus area observes a broad range of event, security configurations, and traffic flow attributes?

A. External Attack Surface
B. Prevent Compromise
C. Data Loss
D. Lateral Propagation

Answer: B

NEW QUESTION 7
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 8

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 9
When are users granted conditional access to segmented private applications?

A. After passing criteria checks related to authorization and security.
B. Immediately upon connection request for best performance.
C. After a short delay of a random number of seconds.
D. After verifying the user password inside of private application.

Answer: A

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
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 15
A user is accessing a private application through Zscaler with SSL Inspection enabled. Which certificate will the user see on the browser session?

A. No certificate, as the session is decrypted by the Service Edge
B. A self-signed certificate from Zscaler
C. Real Server Certificate
D. Zscaler generated MITM Certificate

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
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 21
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 26
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 31
What does an Endpoint refer to in an API architecture?

A. An end-user device like a laptop or an OT/IoT device
B. A URL providing access to a specific resource
C. Zscaler public service edges
D. Zscaler API gateway providing access to various components

Answer: B

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 36
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 Mai ware
C. Create Zero Trust Network Decoy
D. Remove External Collaborators and Sharable Link

Answer: D

NEW QUESTION 41
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 43
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 48
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 53
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 55
An administrator needs to SSL inspect all traffic but one specific URL category. The administrator decides to create two policies, one to inspect all traffic and another one to bypass the specific category. What is the logical sequence in which they have to appear in the list?

A. Both policies are incompatible, so it is not possible to have them together.
B. First the policy for the exception Category, then further down the list the policy for the generic "inspect all."
C. First the policy for the generic "inspect all", then further down the list the policy for the exception Category.
D. All policies both generic and specific will be evaluated so no specific order is required.

Answer: B

NEW QUESTION 60
How does Zscaler Risk360 quantify risk?

A. The number of risk events is totaled by location and combined.
B. A risk score is computed based on the number of remediations needed compared to the industry peer average.
C. Time to mitigate each identified risk is totaled, averaged, and tracked to show ongoing trends.
D. A risk score is computed for each of the four stages of breach.

Answer: D

NEW QUESTION 63
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 67
When configuring a ZDX custom application and choosing Type: 'Network' and completing the configuration by defining the necessary probe(s), which performance metrics will an administrator NOT get for users after enabling the application?

A. Server Response Time
B. ZDX Score
C. Client Gateway IP Address
D. Disk I/O

Answer: D

NEW QUESTION 69
Which filtering policy blocked access to the Network Application?

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

Answer: C

NEW QUESTION 72
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 74
What is the default timer in ZDX Advanced for web probes to be sent?

A. 1 minute
B. 10 minutes
C. 30 minutes
D. 5 minutes

Answer: D

NEW QUESTION 76
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 80
Which are valid criteria for use in Access Policy Rules for ZPA?

A. Group Membership, ZIA Risk Score, Domain Joined, Certificate Trust
B. Username, Trusted Network Status, Password, Location
C. SCIM Group, Time of Day, Client Type, Country Code
D. Department, SNI, Branch Connector Group, Machine Group

Answer: A

NEW QUESTION 83
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 88
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 92
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 97
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 102

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 103
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 104
When configuring Applications to be monitored, what probe types can be created?

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

NEW QUESTION 109
Malware Protection inside HTTPS connections is performed using which parts of the Zero Trust Exchange?

A. Deception creating decoy files for malware to discover.
B. Application Segmentation of users to specific private applications.
C. TLS Inspection decrypting traffic to compare signatures for known risks.
D. Data Loss Protection comparing saved filenames for known risks.

Answer: C

NEW QUESTION 113
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 118
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 123
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 124
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 125
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 130
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 131
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 134
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual ZDTA Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the ZDTA Product From:

https://www.2passeasy.com/dumps/ZDTA/

Money Back Guarantee

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