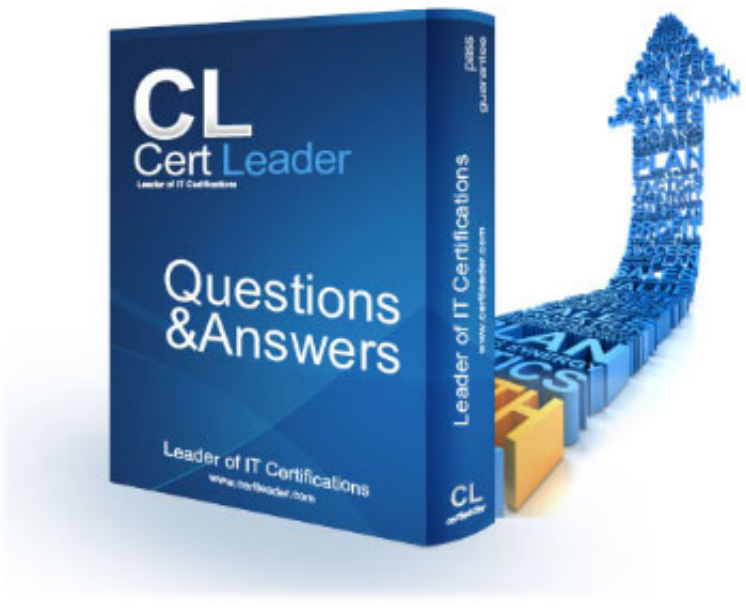
ZDTA Dumps

Zscaler Digital Transformation Administrator

https://www.certleader.com/ZDTA-dumps.html



NEW QUESTION 1
Client Connector forwarding profile determines how we want to forward the traffic to the Zscaler Cloud. Assuming we have configured tunnels (GRE or IPSEC) from locations, what is the recommended combination for on-trusted and off-trusted options?

A. Tunnel v2.0 for on-trusted and tunnel v2.0 for off-trusted
B. None for on-trusted and none for off-trusted
C. None for on-trusted and tunnel v2.0 for off-trusted
D. Tunnel v2.0 for on-trusted and none for off-trusted

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
Which Zscaler forwarding mechanism creates a loopback address on the machine to forward the traffic towards Zscaler cloud?

A. Enforced PAC mode
B. ZTunnel - Packet Filter Based
C. ZTunnel with Local Proxy
D. ZTunnel - Route Based

Answer: C

NEW QUESTION 5
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 6
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 7
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 8
What enables zero trust to be properly implemented and enforced between an originator and the destination application?

A. Trusted network criteria designate the locations of originators which can be trusted.
B. Access is granted without sharing the network between the originator and the destination application.
C. Cloud firewall policies ensure that only authenticated users are allowed access to destination applications.
D. Connectivity between the originator and the destination application is over IPSec tunnels.

Answer: B

NEW QUESTION 9
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 10
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 10
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 13
What is the name of the feature that allows the platform to apply URL filtering even when a Cloud APP control policy explicitly permits a transaction?

A. Allow Cascading
B. Allow and Quarantine
C. Allow URL Filtering
D. Allow and Scan

Answer: A

NEW QUESTION 18
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 22
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 23
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 27
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 30
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 34
In which of the following SaaS apps can you protect data at rest via Zscaler's out-of-band CASB solution?

A. Yahoo Mail
B. Twitter.
C. Google Drive.
D. Facebook.

Answer: C

NEW QUESTION 38
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 42
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 46
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 48
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 51

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 56
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 60
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 65
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 70
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 71
During the authentication process while accessing a private web application, how is the SAML assertion delivered to the service provider?

A. HTTP Redirect on the browser
B. API request/response sequence
C. Through the client connector
D. Form POST via the browser

Answer: D

NEW QUESTION 73
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 76
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your ZDTA Exam with Our Prep Materials Via below:

https://www.certleader.com/ZDTA-dumps.html