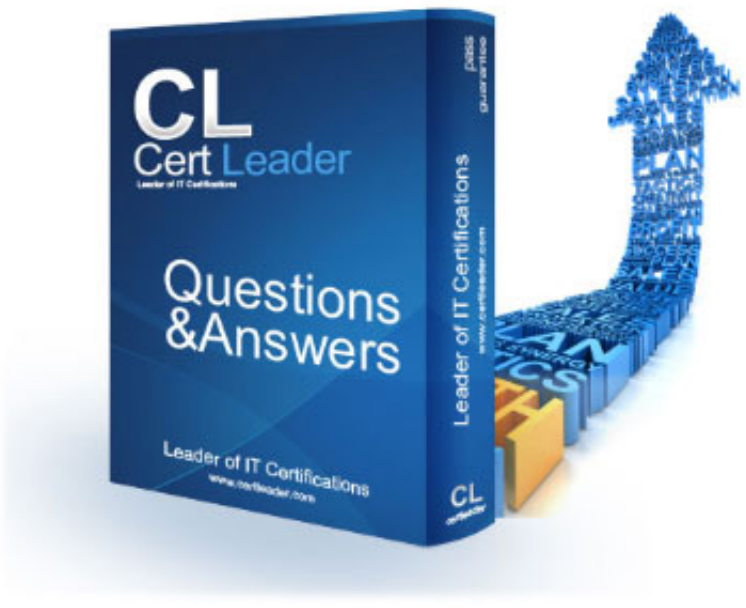
ZDTA Dumps

Zscaler Digital Transformation Administrator

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



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
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 4
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 5
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 6
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 7
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 8

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 9
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 10
How is the relationship between App Connector Groups and Server Groups created?

A. The relationship between Agp_ 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 Agp_ Connector Groups that provide visibility to this Server Group
C. Both Agg Connector Groups and Server Groups are linked together via the Data Center element
D. When you create a new Agg Connector Group you must select the list of Server Groups to which it provides visibility

Answer: B

NEW QUESTION 10
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 15
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 17
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 21
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 22
Which of the following secures all IP unicast traffic?

A. Secure Shell (SSH)
B. Tunnel with local proxy
C. Enforce PAC
D. Z-Tunnel 2.0

Answer: D

NEW QUESTION 25
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 29
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 31
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 36
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 38
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 39
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 40
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 42
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 44
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 46
Which of the following is a key feature of Zscaler Data Protection?

A. Data loss prevention
B. Stopping reconnaissance attacks
C. DDoS protection
D. Log analysis

Answer: A

NEW QUESTION 51
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 Zldentity"s token endpoint.
B. The administrator needs to send a GET request along with the required parameters to Zldentity'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 53
An organization has more than one ZIA instance, each on different clouds. The organization is using the same login domain for both and upon login users are given this menu in ZCC asking which cloud they would like to join. What steps could an Administrator take to avoid having this menu appear?

A. Customize an MSI version of the ZCC file specifying the USERDOMAIN variable.
B. Customize an MSI version of the ZCC file specifying the CLOUDNAME variable.
C. Federate the login domain between two different IDP instances.
D. Create only one SAML integration with the desired ZIA instance.

Answer: B

NEW QUESTION 54
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 57
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 61
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 66
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 70
Which of the following DLP components make use of Boolean Logic?

A. DLP Rules
B. DLP Dictionaries
C. DLP Engines
D. DLP Identifiers

Answer: A

NEW QUESTION 73
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 74
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 75
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 78
Which filtering policy blocked access to the Network Application?

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

Answer: C

NEW QUESTION 83

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

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

Answer: C

NEW QUESTION 85
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 87
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 88
An administrator would like users to be able to use the corporate instance of a SaaS application. Which of the following allows an administrator to make that distinction?

A. Out-of-band CASB
B. Cloud application control
C. URL filtering with SSL inspection
D. Endpoint DLP

Answer: B

NEW QUESTION 92
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 94
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 98
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 100
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 defaul
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 neede
G. The rise of HTTPS leads renders URL Filtering ineffective as all traffic is encrypted.

Answer: A

NEW QUESTION 102
Is SCIM required for ZIA?

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

Answer: C

NEW QUESTION 107
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 111
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 115
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 118
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 119
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 123

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 127
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 132
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 135
You recently deployed an additional App Connector to and existing app connector group. What do you need to do before starting the zpa-connector service?

A. Copy the group provisioning key to /opt/zscaler/var/provision key
B. Monitor the peak CPU and memory utilization of the AC
C. Schedule periodic software updates for the agg connector group
D. Check the status of the new App Connector in the administration portal

Answer: A

NEW QUESTION 139
FILL IN THE BLANK
Which of the following is an open standard used to provide automatic updates of a user's group and department information?
A Import

A. LDAP Sync
B. SCIM
C. SAML

Answer: C

NEW QUESTION 140
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 142
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 144
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 149
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 152
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 156
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 158
What ports and protocols are forwarded to the Zero Trust Exchange when Zscaler Client Connector is using Tunnel 2.0?

A. TCP ports 80, 443 and 8080 only.
B. Any HTTP/HTTPS traffic as well as DNS.
C. All TCP and UDP ports as well as ICMP traffic.
D. All Web ports as well as FTP and SSH.

Answer: C

NEW QUESTION 160
.....

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