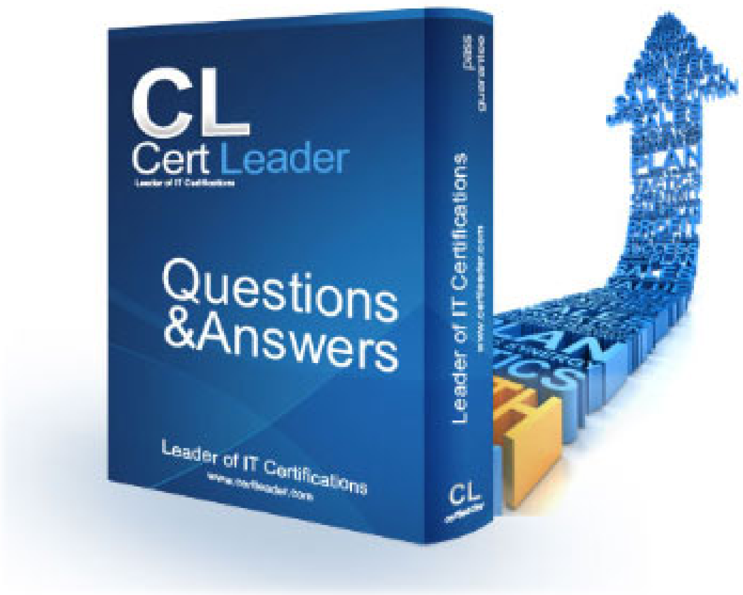
ZDTA Dumps

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
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 3
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 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
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 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
What are the two types of Alert Rules that can be defined?

A. ThreatLabZ pre-defined and customer defined
B. Snort defined and 3rd party defined
C. ThreatLabZ pre-defined and 3rd party defined
D. Customer defined and 3rd party defined

Answer: A

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
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
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 13
How do Access Policies relate to the Application Segments and Application Segment Groups?

A. When a condition is met, an Access Policy can either allow or block access to Application Segments OR Application Segment Groups.
B. When a condition is met, an Access Policy can allow access to Application Segments Groups and block access to Application Segment.
C. When a condition is me
D. an Access Policy can either allow or block access to Application Segments and Application Segment Groups.
E. When a condition is met, an Access Policy can allow access to Application Segments and block access to Application Segment Groups.

Answer: C

NEW QUESTION 18
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 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 24
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 29
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 32
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 35
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 36
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 39
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 42
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 45
Which of the following statements most accurately describes Zero Trust Connections?

A. They require that SSH inspection be enabled.

B. They are dependent on a fixed / static network environment.
C. They are independent of any network for control or trust.
D. They require IPV6.

Answer: C

NEW QUESTION 48
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 50
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 51
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 54
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 56
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 60
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 61
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 66
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 69
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 73
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 78
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 83
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 86
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 89
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 91
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 92
What is the main purpose of Sandbox functionality?

A. Block malware that we have previously identified
B. Build a test environment where we can evaluate the result of policies
C. Identify Zero-Day Threats
D. Balance thread detection across customers around the world

Answer: C

NEW QUESTION 93
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 94
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 96
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 101
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 106
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 110
What does a DLP Engine consist of?

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

Answer: C

NEW QUESTION 113
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 118
While troubleshooting a user's slow application access, can a ZDX administrator see degradations in Wi-Fi signal strength?

A. Yes, the Wi-Fi hop latency is shown on a cloud path probe.
B. Ye
C. but the current Wi-Fi signal strength is only displayed when doing a deep trace.
D. No, ZDX only works on hardwired devices.
E. Yes, a low Wi-Fi signal may be seen in either the results of a Cloud Path Probe or in the device health Wi-Fi signal indicator.

Answer: D

NEW QUESTION 121
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 126
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 131
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 136
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 140
......

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