Zscaler

Exam Questions ZDTA

Zscaler Digital Transformation Administrator

NEW QUESTION 1
What conditions can be referenced for Trusted Network Detection?

A. Hostname Resolution, Network Adapter IP, Default Gateway
B. DNS Servers, DNS Search Domain, Network Adapter IP
C. Hostname Resolution, DNS Servers, Geo Location
D. DNS Search Domain, DNS Server, Hostname Resolution

Answer: D

NEW QUESTION 2
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 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
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 5
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 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 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 8
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 9
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
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 10
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 12
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 17
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 19
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 22
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 23
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 24
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 28
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 33
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 35
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 39
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 41
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 44
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 46
Which of the following are correct request methods when configuring a URL filtering rule with a Caution action?

A. Connect, Get, Head
B. Options, Delete, Put
C. Get, Delete, Trace
D. Connect, Post, Put

Answer: A

NEW QUESTION 51
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 54
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 57
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 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 62
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 66
Which filtering policy blocked access to the Network Application?

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

Answer: C

NEW QUESTION 68
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 70
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 71
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 72
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 76
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 79
Is SCIM required for ZIA?

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

Answer: C

NEW QUESTION 83
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 85
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 86
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 91
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 95
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 96
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 99
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 104
Which of the following connects Zscaler users to the nearest Microsoft 365 servers for a better experience?

A. Single DNS resolver with forwarders providing centralized results
B. Private MPLS in each branch office providing connection
C. Multiple distributed DNS resolvers providing local results
D. Optimized TCP Scaling for maximum throughput of files

Answer: C

NEW QUESTION 108
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 111
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 115
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 118
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 120
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 121
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 122
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 126
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 128
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 133
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 138
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 142
Which of the following components is installed on an endpoint to connect users to the Zero Trust Exchange regardless of their location - home, work, while traveling, etc.?

A. Client connector
B. Private Service Edge
C. IPSec/GRE Tunnel
D. App Connector

Answer: A

NEW QUESTION 145
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 150
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 153

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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