Zscaler

Exam Questions ZDTA

Zscaler Digital Transformation Administrator

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
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 3
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 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
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 6
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 7
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 8
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 9
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 10
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 10
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 14
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 18
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 19
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 20
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 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 26
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 30
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
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 ZIdentity"s token endpoint.
B. The administrator needs to send a GET request along with the required parameters to ZIdentity'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 37
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 42
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 45
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 47
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 49
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 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 57
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 58
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 62
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 66
What are the two types of Probe supported in ZDX?

A. Web Probes and Cloud Path Probes
B. Application Probes and Network Probes
C. Page Speed Probes and Connection Speed Probes
D. SSaas Probes and Router Probes

Answer: A

NEW QUESTION 68
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 72
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 77
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 78
Which filtering policy blocked access to the Network Application?

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

Answer: C

NEW QUESTION 80
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 84
Which type of malware is specifically used to deliver other malware?

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

Answer: C

NEW QUESTION 88
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 92

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 93
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 96
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 98
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 102
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 104
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 106
The Security Alerts section of the Alerts dashboard has a graph showing what information?

A. Top 5 Malware Programs Detected
B. Top 5 Viruses by Region
C. Top 5 Threats by Systems Impacted
D. Top 5 Unified Threat Yara Options

Answer: C

NEW QUESTION 110
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 114
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 116
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 118
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 121
What does a DLP Engine consist of?

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

Answer: C

NEW QUESTION 123
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 126
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 129
Which of the following is a unified management console for internet and SaaS applications, private applications, digital experience monitoring and endpoint agents?

A. identity Admin Portal
B. Mobile Admin Portal
C. Experience Center

D. One API

Answer: C

NEW QUESTION 133
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 134
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 135
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 138
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 143
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 146
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 148
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 151
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