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
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 3
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 4
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 5
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 6
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 7
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 8
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 9
What is the ZIA feature that ensures certain SaaS applications cannot be accessed from an unmanaged device?

A. Tenant Restriction
B. Identity Proxy
C. Out-of-band Application Access
D. SaaS Application Access

Answer: A

NEW QUESTION 10
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 10
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 14
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 17
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 20
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 22
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 27
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 31
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 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 37
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 39
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 44
Which of the following options will protect against Botnet activity using IPS and Yara type content analysis?

A. Command and Control Traffic
B. Ransomware
C. Troians
D. Adware/Spyware Protection

Answer: A

NEW QUESTION 47
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 50
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 54
Which of the following is the preferred method for authentication in a OneAPI environment?

A. OIDC
B. SCIM
C. SAML
D. EntraID

Answer: A

NEW QUESTION 59
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 61
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 65
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 66
What does a DLP Engine consist of?

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

Answer: C

NEW QUESTION 70
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 71
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 72
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 77
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 80
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 83
.....

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

100% Actual & Verified — Instant Download, Please Click
Order The ZDTA Practice Test Here