# 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**
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**
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 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**
What transport mechanism will Zscaler Client Connector use to forward traffic to the Zero Trust Exchange when configured for Tunnel 2.0?

A. Zscaler Client Connector will encapsulate the user's traffic in GRE tunnels to the ZTE.
B. Zscaler Client Connector will encapsulate the user's traffic in IPSec tunnels to the ZTE.
C. Zscaler Client Connector will encapsulate the user's traffic in dTLS/TLS tunnels to the ZTE.
D. Zscaler Client Connector will encapsulate the user's traffic in HTTP Connect tunnels to the ZTE.

**Answer:** C

**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**
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**
You've configured the API connection to automatically download Microsoft Information Protection (MIP) labels into ZIA; where will you use these imported labels to protect sensitive data in motion?

A. Creating a custom DLP Dictionary
B. Creating a SaaS Security Posture Control Policy.
C. Creating a File Type Control Policy.
D. Creating a custom DLP Policy.

**Answer:** D

**NEW QUESTION 9**
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 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**
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 11**
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 13**
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 16**
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 19**
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**
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 26**
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 27**
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 32**
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 36**
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 40**
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 43**
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 48**
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 52**
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 56**
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 60**
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 65**
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 66**
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 69**
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 70**
Which type of malware is specifically used to deliver other malware?

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

**Answer:** C

**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 75**
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 76**
SSH use or tunneling was detected and blocked by which feature?

A. Cloud Agg Control
B. URL Filtering
C. Advanced Threat Protection D Mobile Malware Protection

**Answer:** A

**NEW QUESTION 79**
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 82**
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 87**
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 89**
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 91**
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 95**
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 100**
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 105**
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 106**
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 108**
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 109**
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 114**
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 115**
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 120**
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 123**
.....

# 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