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
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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
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 13
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 14
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 17
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 20
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 23
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 27
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 31
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 36
Zscaler Platform Services works upon unencrypted data from encrypted communications due to which of the following?

A. Antivirus
B. Tenant Restrictions
C. Web Filtering
D. TLS Inspection

Answer: D

NEW QUESTION 39
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 43
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 44
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 47
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 48
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 53
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 56
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 59
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 63
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 64
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 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 67
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 70
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 72
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 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 78
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 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 84
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 85
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 88
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 92
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 96
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 99
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 104
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 105
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 107
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 112
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 117
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 119
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 121
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 126
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 129
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 131
.....

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