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
Which types of Botnet Protection are supplied by Advanced Threat Protection?

A. Malicious file downloads, Command traffic (sending / receiving), Data exfiltration
B. Connections to known C&C servers, Command traffic (sending / receiving), Unknown C&C using AI/ML
C. Connections to known C&C servers, Detection of phishing sites, Access to spam sites
D. Vulnerabilities in web server applications, Unknown C&C using AI/ML, Vulnerable ActiveX controls

Answer: B

NEW QUESTION 3
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 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
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 8
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 9
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 10
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 10
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 15
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 18
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 23
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 27
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 32
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 37
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 40
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 43
How is data gathered with ZDX Advanced client performance?

A. By generating synthetic transactions to designated Internet and Private applications every 5 minutes and measuring the performance of those sessions.
B. By constantly analyzing live user sessions to both Internet and Private applications and measuring the performance of those sessions.
C. By using AI predictive analysis ZDX can extrapolate near-term client performance based upon recent past data observed.
D. By constantly analyzing live user sessions to critical SaaS applications and measuring the performance of those sessions.

Answer: B

NEW QUESTION 44
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 48
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 51
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 56
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 59
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 64
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 68
What does Zscaler Advanced Firewall support that Zscaler Standard Firewall does not?

A. Destination NAT
B. FQDN Filtering with wildcard
C. DNS Dashboards, Insights and Logs
D. DNS Tunnel and DNS Application Control

Answer: D

NEW QUESTION 69
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 73
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 75
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 79
Which of the following is a valid action for a SaaS Security API Data Loss Prevention Rule?

A. Enable AI/ML based Smart Browser Isolation
B. Quarantine Mai ware
C. Create Zero Trust Network Decoy
D. Remove External Collaborators and Sharable Link

Answer: D

NEW QUESTION 81
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 84
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 86
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 89
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 90
Which attack type is characterized by a commonly used website or service that has malicious content like malicious JavaScript running on it?

A. Watering Hole Attack
B. Pre-existing Compromise
C. Phishing Attack
D. Exploit Kits

Answer: A

NEW QUESTION 94
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 96
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 99
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 100
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 101
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 105
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 110
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 114
Which type of malware is specifically used to deliver other malware?

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

Answer: C

NEW QUESTION 116
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 118
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 121
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 122
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 127
As technology that exists for a very long period of time, has URL Filtering lost its effectiveness?

A. URL Filter is the most commonly used web filtering technique in the arsena
B. It acts as first line of defense.
C. In a modern cloud world, access to all Internet sites and cloud applications should be granted by defaul
D. URL Filtering is no longer needed.
E. URL Filtering has been replaced by CASB functionality through blocking access to all Internet sites and only allowing a few corporate applications.
F. URL Filtering is outdated and no longer neede
G. The rise of HTTPS leads renders URL Filtering ineffective as all traffic is encrypted.

Answer: A

NEW QUESTION 129
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 132
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 135
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 137
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 138
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 140
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 144
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 145
You recently deployed an additional App Connector to and existing app connector group. What do you need to do before starting the zpa-connector service?

A. Copy the group provisioning key to /opt/zscaler/var/provision key
B. Monitor the peak CPU and memory utilization of the AC
C. Schedule periodic software updates for the agg connector group
D. Check the status of the new App Connector in the administration portal

Answer: A

NEW QUESTION 147
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 149
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 150
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 155
.....

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