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
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
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 6
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 7
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 8

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 9
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 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 14
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 15
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 17
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 22
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 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 29
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 31
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 34
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 36
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 37
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 39
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 41
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 46
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 49
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 54
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 58
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 63
Zscaler Data Protection supports custom dictionaries.
What actions can administrators take with these dictionaries to protect data in motion?

A. Define specific keywords, phrases, or patterns relevant to their organization's sensitive data policy.
B. Define specific governance and regulations relevant to their organization's sensitive data policy.
C. Define specific SaaS tenant relevant to their organization's sensitive data policy
D. Define specific file types relevant to their organization's sensitive data policy.

Answer: A

NEW QUESTION 68
Which Advanced Threat Protection feature restricts website access by geographic location?

A. Spyware Callback
B. Botnet Protection
C. Blocked Countries
D. Browser Exploits

Answer: C

NEW QUESTION 70
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 74
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 77
What is the purpose of the Zscaler Client Connector providing the authentication token to the Zscaler Client Connector Portal after it is received from Zscaler Internet Access?

A. To bypass multifactor authentication (MFA) during the enrollment process
B. To immediately grant the user access to Zscaler Private Access resources
C. To enable the portal to register the user??s device and pass the registration to Zscaler Internet Access
D. To share the authentication token with the SAML IdP to validate the user session

Answer: C

NEW QUESTION 79
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 84
What does a DLP Engine consist of?

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

Answer: C

NEW QUESTION 87
Which is an example of Inline Data Protection?

A. Preventing the copying of a sensitive document to a USB drive.
B. Preventing the sharing of a sensitive document in OneDrive.
C. Analyzing a customer??s M365 tenant for security best practices.
D. Blocking the attachment of a sensitive document in webmail.

Answer: D

NEW QUESTION 89
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 91
When users are authenticated using SAML, what are the two most efficient ways of provisioning the users?

A. Hosted User Database and Directory Server Synchronization
B. SAML and Hosted User Database
C. SCIM and Directory Server Synchronization

D. SCIM and SAML Autoprovisioning

Answer: D

NEW QUESTION 93
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 98
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 100
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 103
.....

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