Zscaler

Exam Questions ZDTA

Zscaler Digital Transformation Administrator

NEW QUESTION 1
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 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
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 4
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 5
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 6
When are users granted conditional access to segmented private applications?

A. After passing criteria checks related to authorization and security.
B. Immediately upon connection request for best performance.
C. After a short delay of a random number of seconds.
D. After verifying the user password inside of private application.

Answer: A

NEW QUESTION 7
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 8
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 9
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 10
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 10
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 14
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 16
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 19
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 23
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 27
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 31
Which type of malware is specifically used to deliver other malware?

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

Answer: C

NEW QUESTION 35
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 39
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 42
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 46
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
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 55
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 58
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 60
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 63
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 65
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 68
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 72
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 76
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 80
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 81
What does TLS Inspection for Zscaler Internet Access secure public internet browsing with?

A. Storing connection streams for future customer review.
B. Removing certificates and reconnecting client connection using HTTP.
C. Intermediate certificates are created for each client connection.
D. Logging which clients receive the original webserver certificate.

Answer: C

NEW QUESTION 85
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 88
.....

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