Zscaler

Exam Questions ZDTA

Zscaler Digital Transformation Administrator

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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
Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS includes which of the following?

A. Spyware Callback
B. Anonymizers
C. Cookie Stealing
D. IRC Tunneling

Answer: C

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
The security exceptions allow list for Advanced Threat Protection apply to which of the following Policies?

A. Sandbox
B. URL Filtering
C. File Type Control
D. IPS Control

Answer: A

NEW QUESTION 5
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 6
Zscaler Client Connector checks for software updates automatically at which interval?

A. Every 6 hours
B. Every 12 hours
C. Every 2 hours
D. Every 24 hours

Answer: C

NEW QUESTION 7
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 8

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 9
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 10
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
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 13
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 15
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 18
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 23
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 25
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 30
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 32
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 35
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 38
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 39
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 42
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 45
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 50
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 51
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 53
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 57
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 58
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 63
Which filtering policy blocked access to the Network Application?

A. Sandbox
B. Browser Control
C. Firewall Filtering
D. DLP

Answer: C

NEW QUESTION 68
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 69
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 70
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 72
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 73
Is SCIM required for ZIA?

A. Depends
B. Maybe
C. No
D. Yes

Answer: C

NEW QUESTION 77
Which of the following DLP Notification methods can be used to forward a copy of the data that triggered the DLP policy to the auditor?

A. Email Notification Template
B. NSS Log Forwarding to SIEM
C. SMS Text Message via PagerDuty
D. Zscaler Client Connector pop-up message

Answer: A

NEW QUESTION 80
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 81
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 82
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 86
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 90
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 95
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 100
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 101
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 106
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 107
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 112
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 115
.....

Relate Links

100% Pass Your ZDTA Exam with Exambible Prep Materials

https://www.exambible.com/ZDTA-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/