EXAMTOPICS
- Expert Verified, Online, **Free**.

CERTIFICATION TEST
- CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

Within ZPA, the mapping relationship between Connector Groups and Server Groups can best be defined as which of the following?

A. Server Groups are configured for Dynamic Server Discovery so that mapped Connector Groups can then DNS resolve individual application Segment Groups.

B. Connector Groups are configured for Dynamic Server Discovery so that mapped Server Groups can DNS resolve and advertise the applications.

C. Connector Groups are configured for Dynamic Server Discovery so that ZPA can steer traffic through the appropriate Server Group.

D. Server Groups are configured for Dynamic Server Discovery so that mapped Connector Groups can DNS resolve and make health checks toward the application.

Suggested Answer: *D*

None

Question #2 *Topic 1*

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.

Suggested Answer: *B*

None

Question #3 *Topic 1*

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 met, an Access Policy can either allow or block access to Application Segments and Application Segment Groups.

D. When a condition is met, an Access Policy can allow access to Application Segments and block access to Application Segment Groups.

Suggested Answer: *C*

None

Question #4 *Topic 1*

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 arsenal. It acts as first line of defense.

B. In a modern cloud world, access to all Internet sites and cloud applications should be granted by default. URL Filtering is no longer needed.

C. URL Filtering has been replaced by CASB functionality through blocking access to all Internet sites and only allowing a few corporate applications.

D. URL Filtering is outdated and no longer needed. The rise of HTTPS leads renders URL Filtering ineffective as all traffic is encrypted.

Suggested Answer: *A*

None

Question #5 *Topic 1*

You need to SSL inspect all traffic but one specific URL category. You decide 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 generic "inspect all", then further down the list the policy for the exception Category.

C. First the policy for the exception Category, then further down the list the policy for the generic "inspect all."

D. All policies both generic and specific will be evaluated so no specific order is required.

Suggested Answer: *C*

None

Question #6 *Topic 1*

How is the relationship between App Connector Groups and Server Groups created?

A. The relationship between App 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 App Connector Groups that provide visibility to this Server Group

C. Both App Connector Groups and Server Groups are linked together via the Data Center element

D. When you create a new App Connector Group you must select the list of Server Groups to which it provides visibility

Suggested Answer: *B*

None

Question #7 *Topic 1*

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.

Suggested Answer: *A*

None

Question #8 *Topic 1*

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.

Suggested Answer: *C*

None

Question #9 *Topic 1*

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.

Suggested Answer: *A*

None

Question #10 *Topic 1*

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.

Suggested Answer: *B*

None

Question #11 *Topic 1*

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).

Suggested Answer: *B*

None

Question #12 *Topic 1*

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. Yes, but the current Wi-Fi signal strength is only displayed when doing a deep trace.

C. No, ZDX only works on hardwired devices.

D. 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.

Suggested Answer: *D*

None

Question #13 *Topic 1*

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

A. Connections to known C&C servers, Detection of phishing sites, Access to spam sites

B. Malicious file downloads, Command traffic (sending / receiving), Data exfiltration

C. Connections to known C&C servers, Command traffic (sending / receiving), Unknown C&C using AI ML

D. Vulnerabilities in web server applications, Unknown C&C using AI ML, vulnerable ActiveX controls

Suggested Answer: *C*

None

Question #14 *Topic 1*

Does the Access Control suite include features that prevent lateral movement?

A. Yes. The Cloud Firewall will detect network segments and provide conditional access.

B. No. The endpoint firewall will detect network segments and steer access.

C. Yes. Controls for segmentation and conditional access are part of the Access Control Services.

D. No. Access Control Services will only control access to the Internet and cloud applications.

Suggested Answer: *C*

None

Question #15 *Topic 1*

From a user perspective, Zscaler Bandwidth Control performs traffic shaping and buffering on what direction(s) of traffic?

A. Outbound traffic is shaped. Inbound or localhost traffic is unshaped.

B. Outbound or inbound traffic is shaped. Localhost traffic is unshaped.

C. Inbound traffic is shaped. Outbound or localhost traffic is unshaped.

D. Localhost traffic is shaped. Outbound or Inbound traffic is unshaped.

Suggested Answer: *A*

None

Question #16 *Topic 1*

How does Zscaler Risk360 quantify risk?

A. A risk score is computed based on the number of remediations needed compared to the industry peer average.

B. A risk score is computed for each of the four stages of breach.

C. The number of risk events is totaled by location and combined.

D. Time to mitigate each identified risk is totaled, averaged, and tracked to show ongoing trends.

Suggested Answer: *B*

None

Question #17 *Topic 1*

What does TLS Inspection for Zscaler Internet Access secure public internet browsing with?

A. Intermediate certificates are created for each client connection.

B. Logging which clients receive the original webserver certificate.

C. Removing certificates and reconnecting client connection using HTTP.

D. Storing connection streams for future customer review.

Suggested Answer: *A*

None

Question #18 *Topic 1*

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.

Suggested Answer: *D*

None

Question #19 *Topic 1*

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.

Suggested Answer: *A*

None

Question #20 *Topic 1*

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.

Suggested Answer: *B*

None

Question #21 *Topic 1*

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.

Suggested Answer: *A*

None

Question #22 *Topic 1*

What mechanism identifies the ZIA Service Edge node that the Zscaler Client Connector should connect to?

A. The PAC file used in the Forwarding Profile

B. The PAC file used in the Application Profile

C. The IP ranges included/excluded in the App Profile

D. The Machine Key used in the Application Profile

Suggested Answer: *A*

None

Question #23 *Topic 1*

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.

Suggested Answer: *C*

None

Question #24 *Topic 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

Suggested Answer: *D*

Community vote distribution

B (100%)

None

Question #25 *Topic 1*

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

Suggested Answer: *D*

None

Question #26 *Topic 1*

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.

Suggested Answer: *C*

None

Question #27 *Topic 1*

Which of the following are types of device posture?

A. Certificate Trust, File Path, Full Disk Encryption

B. Unauthorized Modification, OS Version, License Key

C. Domain Joined, Process Check, Deception Check

D. Detect CrowdStrike, CrowdStrike ZTA score, First name

Suggested Answer: *A*

None

Question #28 *Topic 1*

Which of the following is a common use case for adopting Zscaler's Data Protection?

A. Prevent download of Malicious Files

B. Prevent loss to Internet and Cloud Apps

C. Securely connect users to Private Applications

D. Reduce your Internet Attack Surface

Suggested Answer: *B*

None

Question #29 *Topic 1*

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 hashtag.

Suggested Answer: *A*

None

Question #30 *Topic 1*

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

Suggested Answer: *D*

None

Question #31 *Topic 1*

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 Malware

C. Create Zero Trust Network Decoy

D. Remove External Collaborators and Sharable Link

Suggested Answer: *D*

None

Question #32 *Topic 1*

Which of the following is a feature of ITDR (Identity Threat Detection and Response)?

A. Prevents Patient Zero Infections

B. Reduces identity related risks

C. Prevents connections to Embargoed Countries

D. Blocks malicious traffic by dropping packets

Suggested Answer: *B*

None

Question #33 *Topic 1*

Which of the following is a unified management console for internet and SaaS applications, private applications, digital experience monitoring and endpoint agents?

A. ZIdentity Admin Portal

B. Mobile Admin Portal

C. Experience Center

D. One API

Suggested Answer: *C*

None

Question #34 *Topic 1*

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

Suggested Answer: *D*

None

Question #35 *Topic 1*

Fundamental capabilities needed by other services within the Zscaler Zero Trust Exchange are provided by which of these?

A. Access Control Services

B. Platform Services

C. Digital Experience Monitoring

D. Cyber Security Services

Suggested Answer: *B*

None

Question #36 *Topic 1*

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

Suggested Answer: *C*

None

Question #37 *Topic 1*

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

Suggested Answer: *A*

None

Question #38 *Topic 1*

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

Suggested Answer: *B*

None

Question #39 *Topic 1*

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. Trojans

D. Adware/Spyware Protection

Suggested Answer: *A*

None

Question #40 *Topic 1*

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

Suggested Answer: *D*

None

Question #41 *Topic 1*

Which of the following is an open standard used to provide automatic updates of a user's group and department information?

A. Import

B. LDAP Sync

C. SCIM

D. SAML

Suggested Answer: *C*

None

Question #42 *Topic 1*

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

A. Spyware Callback

B. Botnet Protection

C. Blocked Countries

D. Browser Exploits

Suggested Answer: *C*

None

Question #43 *Topic 1*

SSH use or tunneling was detected and blocked by which feature?

A. Cloud App Control

B. URL Filtering

C. Advanced Threat Protection

D. Mobile Malware Protection

Suggested Answer: *A*

None

Question #44 *Topic 1*

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

Suggested Answer: *A*

None

Question #45 *Topic 1*

Which SaaS platform is supported by Zscaler's SaaS Security Posture Management (SSPM)?

A. Amazon S3

B. Webex Teams

C. Dropbox

D. Google Workspace

Suggested Answer: *D*

None

Question #46 *Topic 1*

What is the default policy configuration setting for checking for Viruses?

A. Allow

B. Block

C. Unwanted Applications

D. Malware Protection

Suggested Answer: *B*

None

Question #47 *Topic 1*

Which of the following is the preferred method for authentication in a OneAPI environment?

A. OIDC

B. SCIM

C. SAML

D. EntraID

Suggested Answer: *A*

None

Question #48 *Topic 1*

Which filtering policy blocked access to the Network Application?

A. Sandbox

B. Browser Control

C. Firewall Filtering

D. DLP

Suggested Answer: *C*

None

Question #49 *Topic 1*

What is the default timer in ZDX Advanced for web probes to be sent?

A. 1 minute

B. 30 minutes

C. 10 minutes

D. 5 minutes

Suggested Answer: *D*

None

Question #50 *Topic 1*

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

Suggested Answer: *A*

None

Question #51 *Topic 1*

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

Suggested Answer: *C*

None

Question #52 *Topic 1*

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.

Suggested Answer: *D*

None

Question #53 *Topic 1*

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

Suggested Answer: *A*

None

Question #54 *Topic 1*

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

Suggested Answer: *C*

None

Question #55 *Topic 1*

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

Suggested Answer: *C*

None

Question #56 *Topic 1*

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

Suggested Answer: *A*

None

Question #57 *Topic 1*

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 an IPS engine, which will detect the evasion techniques and will just block the transactions as it is invalid.

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 Deep Packed Inspection, which detects protocol evasions and sends the traffic to the respective engines for inspection and handling.

Suggested Answer: *D*

None

Question #58 *Topic 1*

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.

Suggested Answer: *C*

None

Question #59 *Topic 1*

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.

Suggested Answer: *C*

None

Question #60 *Topic 1*

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. Saas Probes and Router Probes

Suggested Answer: *A*

None

Question #61 *Topic 1*

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.

Suggested Answer: *B*

None

Question #62 *Topic 1*

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.

Suggested Answer: *C*

None

Question #63 *Topic 1*

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

Suggested Answer: *B*

None

Question #64 *Topic 1*

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

Suggested Answer: *A*

None

Question #65 *Topic 1*

Is SCIM required for ZIA?

A. Depends

B. Maybe

C. No

D. Yes

Suggested Answer: *C*

None

Question #66 *Topic 1*

Which is an example of Inline Data Protection?

A. Preventing the copying of a sensitive document to a USB drive.

B. Analyzing a customer's M365 tenant for security best practices.

C. Blocking the attachment of a sensitive document in webmail.

D. Preventing the sharing of a sensitive document in OneDrive.

Suggested Answer: *C*

None

Question #67 *Topic 1*

Which of the following connects Zscaler users to the nearest Microsoft 365 servers for a better experience?

A. Multiple distributed DNS resolvers providing local results

B. Private MPLS in each branch office providing connection

C. Single DNS resolver with forwarders providing centralized results

D. Optimized TCP Scaling for maximum throughput of files

Suggested Answer: *A*

None

Question #68 *Topic 1*

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

Suggested Answer: *C*

None

Question #69 *Topic 1*

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 app connector group

D. Check the status of the new App Connector in the administration portal

Suggested Answer: *A*

None

Question #70 *Topic 1*

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.

Suggested Answer: *A*

None

Question #71 *Topic 1*

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

Suggested Answer: *A*

None