

Zscaler.ZDTA.v2026-10-08.q118

Exam Code:	ZDTA
Exam Name:	Zscaler Digital Transformation Administrator
Certification Provider:	Zscaler
Free Question Number:	118
Version:	v2026-10-08
# of views:	103
# of Questions views:	1244
https://www.freecram.net/torrent/Zscaler.ZDTA.v2026-10-08.q118.html	

NEW QUESTION: 1

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: ([SHOW ANSWER](#))

Certificate-pinned applications fail when an inspection proxy substitutes a trusted Zscaler certificate for the origin certificate. The application expects the server certificate or public key to match a pinned value and therefore rejects the inspected session. The fastest way to diagnose this is to inspect SSL logs for failed client handshakes, certificate errors, or bypass candidates. Option A (They could look at SSL logs for a failed client handshake) is correct because SSL logs show the handshake failure pattern created by certificate pinning.

Why the other options are incorrect:

- B). They could reboot the endpoint device: Rebooting may clear a local issue, but certificate pinning is a TLS validation problem. Logs are the right first place to confirm the failed handshake.
- C). They could inspect the ZIA Web Policy: ZIA Web Policy controls web access outcomes. A pinned- certificate failure shows up in SSL/TLS handshake behavior, so SSL logs are more direct.
- D). They could look into the SaaS application analytics tab: SaaS analytics show application usage and risk.

They will not show the client TLS handshake failure that reveals certificate pinning.

NEW QUESTION: 2

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: ([SHOW ANSWER](#))

When SSL Inspection policy bypasses a transaction, Zscaler does not decrypt and re-sign the session. Instead, the proxy passes the TLS connection through so the browser receives the real origin-server certificate. This behavior is used for pinned applications, privacy categories, and traffic that should not be decrypted. Option C (When traffic is exempted in SSL Inspection policy rules) is correct because bypassed SSL Inspection rules preserve the server certificate in the user ' s browser session.

Why the other options are incorrect:

A). When traffic contains a known threat signature: Threat signatures trigger security handling such as blocking or inspection. Passing the real server certificate happens when SSL inspection is bypassed.

B). When web traffic is on custom TCP ports: Custom TCP ports affect traffic handling and forwarding. They do not automatically make Zscaler present the real origin certificate to the browser.

D). When user has connected to server in the past: Past connection history does not decide certificate presentation. The SSL Inspection policy action for the current transaction does.

NEW QUESTION: 3

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: ([SHOW ANSWER](#))

At launch, Zscaler Client Connector must determine which tenant and identity flow apply to the user ' s domain. The Zscaler Central Authority provides this discovery information so the client can direct authentication to the correct IdP and service cloud. Option B (Zscaler Central Authority) is correct because Central Authority is the initial lookup point for domain and IdP context.

Why the other options are incorrect:

A). Zscaler Private Access (ZPA) Portal: The ZPA portal manages private access configuration. At launch, Client Connector first needs cloud/domain discovery, which is handled through Central Authority.

C). Zscaler Internet Access (ZIA) Portal: The ZIA portal manages Internet Access policy after tenant selection.

It is not the first discovery service that maps the user domain to the correct IdP.

D). Zscaler Client Connector Portal: Zscaler Client Connector is the endpoint agent that steers traffic, authenticates users, reports posture, and supplies ZDX telemetry.

NEW QUESTION: 4

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: (SHOW ANSWER)

Zscaler DLP separates detection logic from enforcement policy. Dictionaries contain the sensitive-data patterns, keywords, identifiers, regexes, or fingerprinted data that identify protected information. DLP engines use those dictionaries to evaluate content, and DLP rules or policies decide the enforcement action. Option C (DLP engines) is correct because the detection foundation of a DLP engine is the dictionary content it evaluates against traffic or files.

Why the other options are incorrect:

- A). Hosted PAC Files: A PAC file tells the client or browser which proxy path to use for matching destinations.
- B). Index Tool: Index Tool suggests the hashing/indexing utility itself. In Zscaler DLP terminology, the protected content matching object is the IDM/EDM template or dictionary construct named by the answer.
- D). VPN Credentials: VPN credentials authenticate remote network access. They are not a DLP matching method for identifying sensitive documents.

NEW QUESTION: 5

Which of the following is unrelated to the properties of ' Trusted Networks ' ?

- A. DNS Server
- B. Default Gateway
- C. Org ID
- D. Network Range

Answer: C (LEAVE A REPLY)

Trusted Network Detection uses network-observable criteria such as DNS server, DNS search domain, gateway, and network ranges to determine whether the endpoint is on a corporate network. An Org ID is tenant identity, not a network characteristic visible on the endpoint. Option C (Org ID) is correct because Org ID is unrelated to trusted-network properties.

Why the other options are incorrect:

- A). DNS Server: DNS Server criteria identify a trusted network by checking whether the endpoint sees expected internal resolver addresses.
- B). Default Gateway: Default Gateway can identify a local network path, but it is not always one of the exact trusted-network criteria set in this item.

D). Network Range: Network range can describe local addressing, but the tested Trusted Network property set is based on the exact ZCC detection fields in the question.

NEW QUESTION: 6

What role does an App Connector serve?

- A. App Connectors enforce security policies for traffic destined for SaaS applications.
- B. App Connectors enable user experience monitoring for all applications.
- C. App Connectors expose a public IP for users to connect to for private application access.
- D. App Connectors mediate seamless communication for applications, services and data sources.

Answer: ([SHOW ANSWER](#))

An App Connector is the ZPA component that sits near private applications and establishes outbound-only connections to the Zscaler cloud. It brokers application reachability without exposing inbound ports or public IP addresses, allowing users to connect to applications rather than networks. Option D (App Connectors mediate seamless communication for applications, services and data sources) is correct because App Connectors mediate communication to private applications, services, and data sources.

Why the other options are incorrect:

- A). App Connectors enforce security policies for traffic destined for SaaS applications: SaaS applications are handled by ZIA controls such as URL Filtering, Cloud App Control, and DLP, not by ZPA App Connectors.
- B). App Connectors enable user experience monitoring for all applications: User-experience monitoring is ZDX's job. App Connectors provide the outbound broker path that lets users reach private applications.
- C). App Connectors expose a public IP for users to connect to for private application access: Publishing a public IP exposes an attack surface; ZPA avoids that by using inside-out connector connectivity.

NEW QUESTION: 7

A manufacturing firm is merging with a subsidiary that uses a separate identity provider. A ZPA Access Policy for an engineering CAD application uses SCIM groups for authorization. A new administrator authenticates successfully through SAML and presents the Engineering claim, but the subsidiary's SCIM synchronization is delayed, so the administrator does not appear in the expected group in ZIdentity.

Which action should the ZPA administrator take to avoid inconsistent access while preserving auditability?

- A. Reconfigure the policy to use NameID for authorization, accepting reduced traceability of group criteria
- B. Initiate a SCIM resynchronization and validate the user's group membership in ZIdentity, while keeping the Access Policy bound to SCIM groups
- C. Create a local ZIdentity group with provisional engineering membership, accepting drift from the directory of record

D. Change identity-provider routing so the engineer authenticates through the parent company's identity provider, accepting misalignment with the subsidiary's directory mappings

Answer: B ([LEAVE A REPLY](#))

Option B restores consistency between the directory of record and the authorization data that the ZPA policy actually evaluates. Successful SAML authentication proves identity but does not substitute for SCIM group membership when the Access Policy criterion is a SCIM group. The administrator should trigger or correct synchronization, inspect the resulting membership, and review synchronization events before granting access.

Zscaler's SCIM Groups documentation states that these groups are pulled from the identity provider, while SCIM Sync Logs record changes to users, attributes, groups, and memberships for troubleshooting. Keeping the policy bound to SCIM groups preserves role-based intent and an auditable source of truth. NameID is an identity value, not reliable group authorization. A provisional local group creates drift, and rerouting authentication does not repair the subsidiary's authoritative SCIM membership.

NEW QUESTION: 8

Security teams are vetting approaches to private application access across two merging organizations to reduce post-acquisition lateral movement.

Which approach best constrains internal discovery and probing while preserving required connectivity?

A. Adopt ZPA user-to-app segmentation with inside-out connectivity so users reach defined applications and cannot traverse broader IP ranges.

B. Centralize VPN concentrators and restrict subnet access by department to contain exploratory traffic during initial entitlement mapping.

C. Extend shared VLANs across the combined data centers and use access control lists to discourage host- to-host enumeration during audits.

D. Apply IDS signatures at core routing layers to flag port scans and perform rate limiting until both environments complete segmentation.

Answer: ([SHOW ANSWER](#)**)**

Answer A is correct. ZPA brokers a connection between an authorized identity and a specifically defined private application instead of extending network access to the user. App Connectors establish outbound connections to the Zero Trust Exchange, so applications do not require inbound exposure. Zscaler describes this model as a segment of one: users receive least-privileged connectivity to named applications, while unrelated applications and IP ranges remain invisible and unreachable. That directly limits discovery, probing, and lateral movement between the two merging environments while allowing approved business connectivity to continue. VPN concentrators, shared VLANs, and subnet ACLs still place users on routable net works and increase the scope that must be protected. Intrusion detection can report scanning, but it does not remove the underlying reachability. See Zscaler's Private Access data sheet and ZPA cloud architecture.

NEW QUESTION: 9

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: ([SHOW ANSWER](#))

When migrating from an on-premises proxy to Tunnel Mode, leaving legacy browser or system proxy settings in place can create loops or conflicting forwarding paths. Best practice is to enforce no proxy configuration so Client Connector owns traffic steering cleanly through the configured tunnel. Option B (Enforce no Proxy Configuration) is correct because Tunnel Mode should not depend on legacy proxy auto-configuration.

Why the other options are incorrect:

- A). Execute a GPO update to retrieve the proxy settings from AD: A GPO can push Windows settings, but using it to reapply old proxy configuration works against Tunnel Mode best practice.
- C). Use Web Proxy Auto Discovery (WPAD) to auto-configure the proxy: WPAD auto-discovers proxy settings; it can accidentally preserve legacy proxy behavior during a tunnel-mode migration.
- D). Use an automatic configuration script (forwarding PAC file): A PAC file tells the client or browser which proxy path to use for matching destinations.

NEW QUESTION: 10

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

- A. Allow
- B. Block
- C. Unwanted Applications
- D. Malware Protection

Answer: ([SHOW ANSWER](#))

ZIA Malware Protection is an inline security control that blocks malicious files or objects detected through signatures, reputation, and threat-intelligence checks. The policy action must stop the malicious transfer rather than simply route, isolate, or change TLS behavior. Option B (Block) is correct because Block is the malware policy action that prevents the identified malicious content from reaching the user.

Why the other options are incorrect:

- A). Allow: Allow would permit the file or activity. A sandbox or malware policy often needs to hold, block, or analyze suspicious content instead of simply allowing it.
- C). Unwanted Applications: Unwanted Applications is a software/category control. Malware-policy behavior is about malicious content handling.
- D). Malware Protection: Malware Protection blocks known malicious objects. Sandbox behavior is used when a file needs detonation or verdict analysis.

NEW QUESTION: 11

Administrators report that some non-compliant devices can still reach private applications. A broad Allow rule precedes device-posture checks in the policy set.

What is the most appropriate next step to satisfy the compliance-before-access requirement?

- A. Broaden URL Filtering blocks for high-risk categories to curtail non-business browsing on those devices
- B. Apply stricter user-group scoping to limit access for departments with higher incident rates
- C. Increase time-based restrictions on access windows to reduce exposure during off-hours
- D. Reorder the policy so posture-based access rules are evaluated before any general Allow statements

Answer: ([SHOW ANSWER](#))

The broad Allow rule is shadowing the posture-dependent decision. Zscaler's Access Policy documentation describes rules that combine users with applications or segment groups, and ZPA evaluates applicable rules according to policy order. A general rule that matches first can grant access without requiring the device to satisfy the intended posture condition. Moving the posture-based rules above the broad Allow ensures compliant devices receive the appropriate access decision and non-compliant devices fall through to a block or a more restrictive rule. The administrator should then test both compliant and non-compliant endpoints and confirm the matched rule in diagnostics. URL Filtering governs internet destinations, not authorization to private ZPA applications. User-group and time restrictions can reduce scope but do not establish device compliance. Option D directly restores the required compliance-before-access evaluation.

NEW QUESTION: 12

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 Wi-Fi signal
- C. Comprehensive URL categories for newly registered domains
- D. Preventing the download of a password protected zip file

Answer: ([SHOW ANSWER](#))

Advanced Threat Protection focuses on security outcomes such as blocking phishing, malicious destinations, C2 callbacks, suspicious files, and exploit activity. A CEO's Teams call suffering because of low Wi-Fi signal is a digital-experience problem, not an ATP workflow event. Option B (Reporting high latency from the CEO's Teams call due to a low Wi-Fi signal) is correct because Wi-Fi latency belongs to ZDX troubleshooting, not ATP.

Why the other options are incorrect:

- A). IPS coverages for client-side and server-side: IPS inspects traffic inline for exploit signatures and attack patterns, then blocks or resets offending sessions.

- C). Comprehensive URL categories for newly registered domains: Newly registered domain categories are part of ATP threat coverage, so they belong in the ATP workflow rather than being the exception.
- D). Preventing the download of a password protected zip file: Blocking password-protected ZIP downloads is a threat-protection control because encrypted archives can hide malware from inspection. It is part of ATP- style enforcement, not the non-ATP item.

NEW QUESTION: 13

Which of the following is a benefit of tunneling?

- A. Increased latency.
- B. Enhanced data security.
- C. Support for only TCP/IP traffic.
- D. Increased header size.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

Enhanced data security is the only listed benefit, so B is correct. A secure tunnel protects traffic as it travels between the endpoint or customer location and the Zscaler service. For example, Zscaler Client Connector uses mutually authenticated TLS-based Z-Tunnels, while locations can use IPsec when encrypted site forwarding is required. Tunneling also provides a controlled path through which Zscaler can apply inspection, access, firewall, and logging policies consistently. Increased latency and additional encapsulation headers are possible operational costs rather than security benefits. Tunneling is also not inherently limited to only TCP /IP in the narrow sense suggested by C; Z-Tunnel 2.0 can forward TCP, UDP, and ICMP traffic. Zscaler describes a Z-Tunnel as a TLS-encrypted, mutually authenticated connection, directly supporting the security benefit.

NEW QUESTION: 14

An organization experiences frequent changes in team structure and wants to keep group membership and access aligned consistently.

Which approach supports scalable, controlled administration?

- A. Rely on SAML assertions to grant administrator rights during authentication events
- B. Consume SCIM-provisioned groups from the identity provider and drive entitlements through those groups
- C. Assign administrative capabilities individually to each user to avoid group-level drift
- D. Create local user accounts to separate access from external directories

Answer: ([SHOW ANSWER](#))

SCIM is designed to automate identity and group lifecycle changes between the authoritative identity provider and Zscaler. Zscaler's SCIM documentation identifies roles and entitlements among the attributes that can be associated with users, while entitlement assignment guidance supports assigning administrative or service entitlements to user groups. Option B therefore

allows team membership changes made at the IdP to flow into the relevant Zscaler groups, where group-based entitlements consistently govern access. SAML primarily supplies authentication assertions during sign-in and is not a substitute for proactive lifecycle provisioning. Individual assignments create administrative overhead and entitlement drift as teams change. Local accounts further separate Zscaler access from the organization's authoritative directory and make joiner, mover, and leaver governance harder to maintain.

NEW QUESTION: 15

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 (LEAVE A REPLY)

A user risk score is an adaptive signal used to tune security policy around individual user exposure. It does not by itself prove compromise, but it helps administrators identify risky users and apply stronger monitoring, access restrictions, or control requirements. Option C (Configure stronger user-specific policies to monitor & control user-level risk exposure) is correct because the value of the score is operational: it supports stronger user-specific policies and risk-based monitoring.

Why the other options are incorrect:

- A). Compare the user risk score with other companies to evaluate users vs other companies: Benchmarking users against other companies would be an executive comparison metric. User risk score is used inside the tenant to tune user-level controls.
- B). Determine whether or not a user is authorized to view unencrypted data: Access to unencrypted data is a data-handling and policy decision. User risk score measures user exposure and behavior risk; it is not a decryption authorization switch.
- D). Determine if a user has been compromised: A high user risk score can indicate suspicious behavior, but it is not a definitive compromise verdict. Administrators use it to strengthen monitoring and policy first.

NEW QUESTION: 16

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: (SHOW ANSWER)

Zscaler OneAPI uses OAuth-style token acquisition through ZIdentity. The administrator or automation client sends a POST request with required parameters such as client credentials to the ZIdentity token endpoint, then uses the returned access token for API calls. Option A (The administrator needs to send a POST request along with the required parameters to ZIdentity 's token endpoint) is correct because token retrieval is performed by POSTing to the ZIdentity token endpoint.

Why the other options are incorrect:

B). The administrator needs to send a GET request along with the required parameters to ZIdentity 's token endpoint: A GET request retrieves resources; it is not used to submit client credentials to the OAuth token endpoint.

C). The administrator needs to logon to the ZIA portal to generate the access token with Super Admin role:

The ZIA portal manages Internet Access policy and service configuration, not the unified identity or OneAPI token endpoint workflow unless the stem says so.

D). The administrator needs to logon to the ZIA portal to generate the access token with API Admin role: The ZIA portal manages Internet Access policy and service configuration, not the unified identity or OneAPI token endpoint workflow unless the stem says so.

Valid ZDTA Dumps shared by EduDump.com for Helping Passing ZDTA Exam!

EduDump.com now offer the **newest ZDTA exam dumps**, the EduDump.com ZDTA exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ZDTA dumps with Test Engine here:

<https://www.edudump.com/exams/Zscaler/ZDTA/premium/> (275 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 17

A regional hospital must provide a vendor with intermittent access to a legacy device-management application hosted on two on-premises servers. The vendor's previous VPN caused noisy port scans to appear in logs and exposed nearby subnets to probing.

Which action should the administrator take to constrain access to the application while reducing lateral movement?

A. Create ZPA Application Segments for the device-management FQDNs and ports, and enforce identity- and posture-based policies for the vendor group

B. Configure DNS sinkholes to divert off-port vendor traffic and apply URL Filtering to suppress non- application flows

C. Deploy a dedicated VLAN and a jump host near the application, and restrict traffic with subnet ACLs that limit the vendor to the jump host's IP address

D. Implement host-based firewall rules on both servers and advertise a reduced VPN route set to the vendor client

Answer: ([SHOW ANSWER](#))

ZPA grants access to defined applications instead of placing the vendor on the hospital network. Zscaler's application documentation defines an application by FQDN or IP address and the required ports. Creating segments for only the two device-management endpoints prevents the vendor from receiving routable access to neighboring subnets. The ZPA Access Policy can then restrict those segments to the vendor identity group and require an acceptable device posture, with explicit time or reauthentication controls for intermittent access. DNS sinkholes and URL Filtering do not provide private-application authorization. A jump host and VLAN reduce exposure but still extend network-level connectivity and add infrastructure to manage. Narrower VPN routes and host firewalls remain network-centric and can still expose reachable services.

Option A provides application-specific, least-privilege access and directly limits lateral movement.

NEW QUESTION: 18

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

Answer: ([SHOW ANSWER](#))

ZDX Score is a normalized digital-experience score used to represent how well a user or application is performing. It is expressed on a 1-to-100 scale, making degraded application, network, and endpoint experience easy to compare across users, locations, and time windows. Option A (1-100) is correct because 1-100 is the ZDX scoring range.

Why the other options are incorrect:

- B).** 1-10: A 1-10 scale is too coarse for ZDX. ZDX uses a 1-100 score so administrators can see more granular experience changes.
- C).** 1 - 1000: A 1-1000 scale would imply excessive precision that ZDX does not present. The product score is the simpler 1-100 user-experience scale.
- D).** 0 - 50: A 0-50 range is not the ZDX scale. ZDX scores are represented on a 1-100 scale.

NEW QUESTION: 19

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** ([LEAVE A REPLY](#))

In API architecture, an endpoint is the URL or URI where a client sends a request to access a specific resource or operation. It is not an end-user device or a Zscaler service edge; it is the addressable API resource exposed through the API system. Option B (A URL providing access to a specific resource) is correct because an API endpoint is a URL providing access to a specific resource.

Why the other options are incorrect:

A). An end-user device like a laptop or an OT/IoT device: A laptop or OT/IoT device is a network endpoint, not an API endpoint.

C). Zscaler public service edges: A Zscaler Service Edge enforces traffic policy; it is infrastructure, not the API resource URL itself.

D). Zscaler API gateway providing access to various components: An API gateway brokers and controls API traffic, while an endpoint is the specific resource path being called.

NEW QUESTION: 20

Your company has a new ZIA subscription. Which is the most effective and secure method of provisioning users?

- A. Kerberos
- B. SAML auto-provisioning
- C. LDAP synchronization
- D. Zscaler Authentication Bridge

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

SAML auto-provisioning is the best answer among the listed methods. When a user authenticates, ZIA can use attributes in the SAML assertion to create the user and populate associated group and department information automatically. This avoids maintaining a separate hosted user database and eliminates the direct LDAP connectivity required by traditional directory synchronization. Kerberos is primarily an authentication mechanism and does not provide the required cloud user-provisioning workflow. LDAP synchronization and Zscaler Authentication Bridge can provision directory information, but they require additional infrastructure and directory integration. Zscaler documents that SAML auto-provisioning enables the service to retrieve user, group, and department information during SAML authentication. For the choices presented, it supplies the most direct and secure cloud-oriented provisioning method.

NEW QUESTION: 21

Company A acquires Company B. Users from both companies require reliable access to internet and SaaS services and to each other's private applications across overlapping RFC1918 address ranges. A legacy VPN retained temporarily for a third-party integration causes intermittent route conflicts and noticeable latency.

Which action should the administrator prioritize to stabilize access and minimize network-level collisions?

- A.** Move all private-application traffic to a shared MPLS core and rely on centralized firewalls to normalize traffic while retaining split tunneling for internet access
- B.** Expand the legacy VPN mesh, tighten BGP route filters, and defer access transformation until IP renumbering is complete
- C.** Onboard private applications into ZPA using application segments and dedicated App Connector groups for each environment, enable Client Connector forwarding for private access, and use ZIA with local internet breakouts, Bandwidth Control, and Microsoft 365 optimization
- D.** Implement SD-WAN steering policies to pin traffic to preferred links and use access control lists to block disallowed subnets as an interim control

Answer: ([SHOW ANSWER](#))

Option C removes user access from the conflicting network-routing model. ZPA connects authorized users to defined applications rather than placing them onto either company's network, so overlapping RFC1918 ranges do not require immediate network convergence or extensive NAT. Separate application segments and App Connector groups preserve environmental boundaries and allow policy to select the correct application path.

Zscaler's M & A architecture guide identifies overlapping address space as a major legacy-integration problem and recommends application-level ZTNA. Zscaler also explains that network abstraction makes overlapping addressing irrelevant for user-to-application access. ZIA local breakout avoids unnecessary backhaul for internet and SaaS traffic. MPLS, additional VPN meshing, BGP filtering, and SD-WAN steering remain network-centric and retain route collisions, operational complexity, or latency.

NEW QUESTION: 22

An administrator suspects that users in Europe are being routed to a distant service edge, inflating latency before traffic reaches a SaaS provider.

Which ZDX diagnostic provides evidence of inefficient client-to-service-edge routing?

- A.** Audit alerting thresholds for regional score drops and assume that the trigger implies service-edge misalignment
- B.** Check endpoint CPU and memory telemetry to argue that device constraints are producing perceived routing inefficiencies
- C.** Review Page Fetch Time graphs for the application and deduce that service-edge selection is suboptimal based on slow loads
- D.** Examine CloudPath probes for the client-to-service-edge leg to verify latency spikes and excessive hop counts

Answer: ([SHOW ANSWER](#))

CloudPath supplies path-level evidence rather than an indirect symptom. Zscaler's CloudPath evaluation documentation shows that the diagnostic presents the network path and reports latency, packet loss, and jitter across hops. Examining the early client-to-Zscaler portion reveals whether European users take an unexpectedly long route, encounter excessive hops, or accumulate latency before reaching the service edge.

That directly tests the routing hypothesis and helps separate local, ISP, Zscaler-edge, and downstream SaaS segments. Alert thresholds can reveal that experience degraded but cannot prove the path was inefficient.

CPU and memory telemetry tests endpoint-resource causes, not service-edge selection. Page Fetch Time confirms application slowness at a high level, yet many application, server, and network factors influence it.

CloudPath is therefore the defensible diagnostic for locating where path delay begins.

NEW QUESTION: 23

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.

Answer: ([SHOW ANSWER](#))

For modern SaaS and web applications, Cloud Application policies usually provide more precise access control than broad URL categories. They can distinguish applications and activities rather than treating the destination as only a URL category. Option A (Cloud Application policies provide better access control) is correct because Cloud Application policies provide deeper application-aware control.

Why the other options are incorrect:

- B). URL filtering policies provide better access control: URL Filtering controls web destinations by category, URL, risk, and action such as allow, block, caution, or isolate.
- C). Wherever possible URL policies are recommended: URL policies are still useful for category-based web filtering. For SaaS applications, Cloud Application policies provide richer application and activity awareness.
- D). Both provide the same filtering capabilities: The two policy types are not equivalent. URL Filtering is destination/category focused, while Cloud App Control understands SaaS apps and actions.

NEW QUESTION: 24

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

- A. The IP ranges included/excluded in the App Profile
- B. The PAC file used in the Forwarding Profile
- C. The PAC file used in the Application Profile
- D. The Machine Key used in the Application Profile

Answer: ([SHOW ANSWER](#))

The PAC file associated with the Forwarding Profile helps Zscaler Client Connector identify how traffic should be forwarded and which ZIA Service Edge path should be used. The App Profile

assigns the Forwarding Profile, but the forwarding PAC is the mechanism that drives service-edge selection logic for ZIA traffic. Option B (The PAC file used in the Forwarding Profile) is correct because the Forwarding Profile PAC is the relevant steering mechanism.

Why the other options are incorrect:

A). The IP ranges included/excluded in the App Profile: App Profile include/exclude ranges influence what traffic the client should handle. The question asks how the ZIA Service Edge is identified, which comes from the forwarding PAC logic.

C). The PAC file used in the Application Profile: A PAC file tells the client or browser which proxy path to use for matching destinations.

D). The Machine Key used in the Application Profile: A machine key identifies the installed device/client context; it is not the PAC/service-edge steering mechanism.

NEW QUESTION: 25

What is the primary function of the on-premises VM in the EDM process?

A. To local analyze cloud transactions for potential PII exfiltration.

B. To replicate sensitive data across all organizational servers.

C. To automate the indexing process by creating hashes for structured data elements.

D. To store sensitive data securely and prevent unauthorized data access.

Answer: (SHOW ANSWER)

Exact Data Match protects structured sensitive data by converting source values into secure hashes before they are used by Zscaler cloud enforcement. The on-premises EDM VM performs indexing locally so raw customer data is not uploaded into the Zscaler cloud. Only hashed values are used for matching. Option C (To automate the indexing process by creating hashes for structured data elements) is correct because the VM automates indexing and sends hashed data, not clear sensitive records, to the cloud.

Why the other options are incorrect:

A). To local analyze cloud transactions for potential PII exfiltration: Local analysis of cloud transactions describes inline inspection behavior. EDM's on-premises VM is used before enforcement to hash/index structured data safely.

B). To replicate sensitive data across all organizational servers: Replicating sensitive data everywhere would increase exposure. EDM avoids sending raw sensitive structured data to Zscaler by hashing/indexing it locally.

D). To store sensitive data securely and prevent unauthorized data access: Secure storage is a general data- security objective. The EDM VM's job is not to become a vault; it prepares hashed indexes for matching.

NEW QUESTION: 26

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: ([SHOW ANSWER](#))

ZPA Access Policy rules use identity, user/group, device posture, and contextual signals to decide private- application access. Valid criteria are enforcement attributes that ZPA can evaluate, such as group membership, risk score, domain-joined state, and certificate trust. Option A (Group Membership, ZIA Risk Score, Domain Joined, Certificate Trust) is correct because all listed criteria are legitimate policy inputs for ZPA access decisions.

Why the other options are incorrect:

B). Username, Trusted Network Status, Password, Location: Trusted Network detection decides whether the device is on a known corporate network using signals such as DNS servers, search domains, gateways, or hostname resolution.

C). SCIM Group, Time of Day, Client Type, Country Code: SCIM provisions and synchronizes users, groups, and attributes between an identity provider and Zscaler.

D). Department, SNI, Branch Connector Group, Machine Group: Machine Group is used for machine identity grouping in some policy contexts, but it is not the same as the listed posture or access criteria set.

NEW QUESTION: 27

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: ([SHOW ANSWER](#))

DLP notification templates can send evidence to the right reviewer or auditor when a policy is triggered. An email notification template is the mechanism that can include or forward a copy of the data that matched the DLP rule, depending on policy configuration and privacy requirements. Option A (Email Notification Template) is correct because it is the DLP notification method used for auditor review.

Why the other options are incorrect:

B). NSS Log Forwarding to SIEM: NSS forwarding sends logs to a SIEM for analysts. End-user DLP coaching or notification is handled by user-facing notification/workflow channels.

C). SMS Text Message via PagerDuty: PagerDuty SMS alerts are operations notifications. The DLP user- notification method in the question is meant to inform or coach the user directly.

D). Zscaler Client Connector pop-up message: Zscaler Client Connector is the endpoint agent that steers traffic, authenticates users, reports posture, and supplies ZDX telemetry.

NEW QUESTION: 28

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: ([SHOW ANSWER](#))

ZIA Malware Protection is an inline security control that blocks malicious files or objects detected through signatures, reputation, and threat-intelligence checks. The policy action must stop the malicious transfer rather than simply route, isolate, or change TLS behavior. Option A (Malware protection) is correct because Block is the malware policy action that prevents the identified malicious content from reaching the user.

Why the other options are incorrect:

- B). File reputation: File reputation checks whether an object is known good or bad. The question's answer is about the behavior-analysis control for unknown files.
- C). SHA-256 hashing: SHA-256 hashing is a cryptographic integrity/hash function. It does not execute a suspicious file or observe behavior the way Cloud Sandbox does.
- D). Site reputation: Site reputation scores web destinations. It does not detonate or analyze the file itself.

NEW QUESTION: 29

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: ([SHOW ANSWER](#))

When trusted corporate locations already forward traffic through GRE or IPSec tunnels, Client Connector should not create a second tunnel on top of the location tunnel while the device is on the trusted network. Off trusted network, however, the client must create its own Tunnel 2.0 path to the Zero Trust Exchange. Option C (None for on-trusted and tunnel v2.0 for off-trusted) is correct because the recommended combination is None on trusted and Tunnel 2.0 off trusted.

Why the other options are incorrect:

- A). Tunnel v2.0 for on-trusted and tunnel v2.0 for off-trusted: Tunnel v2.0 on a trusted network would duplicate forwarding when GRE/IPSec tunnels already steer location traffic to Zscaler. On trusted networks, the client should not build another tunnel.
- B). None for on-trusted and none for off-trusted: None/None leaves Client Connector without tunnel forwarding on both trusted and untrusted networks. That defeats the intended traffic steering design.

D). Tunnel v2.0 for on-trusted and none for off-trusted: Tunnel v2.0 on trusted and none off trusted reverses the desired behavior. Remote/off-trusted users need Client Connector tunneling; trusted locations already use GRE/IPSec.

NEW QUESTION: 30

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: (SHOW ANSWER)

The ZDTA study guide frames common breaches around a four-step lifecycle: discover the attack surface, compromise an entry point, move laterally, and exfiltrate data. Finding the attack surface is the reconnaissance phase in which attackers search for exposed VPNs, firewalls, applications, ports, or public services. Option D (Find Attack Surface) is correct because attack-surface discovery is one of the documented stages.

Why the other options are incorrect:

- A). Find Cash Safe: That phrase describes a physical-world target, not a step in the cyberattack lifecycle.
- B). Find Email Addresses: Email and webhooks forward alerts to people or third-party systems for response workflows.
- C). Find Least Secure Office Building: That phrase describes a physical-world target, not a step in the cyberattack lifecycle.

NEW QUESTION: 31

Which type of attack plants malware on commonly accessed services?

- A. Remote access trojans
- B. Phishing
- C. Exploit kits
- D. Watering hole attack

Answer: (SHOW ANSWER)

A watering-hole attack compromises a legitimate website or service that the intended victims already trust and commonly visit. The attacker plants malicious active content, such as injected JavaScript or exploit code, so users are infected during normal browsing instead of being lured to an obviously suspicious site. The answer is Option D (Watering hole attack) because it specifically describes malware hosted on a commonly accessed service, which is the defining trait of this attack type.

Why the other options are incorrect:

- A). Remote access trojans: A remote access trojan gives an attacker interactive control over a compromised host after infection.

- B). Phishing: Phishing starts with social engineering: fake messages, links, or login pages. The question describes a legitimate common website being seeded with malicious JavaScript.
- C). Exploit kits: Exploit kits automate exploitation after a victim reaches malicious content. They can be used inside an attack chain, but the scenario is naming the watering-hole delivery pattern.

Valid ZDTA Dumps shared by EduDump.com for Helping Passing ZDTA Exam!

EduDump.com now offer the **newest ZDTA exam dumps**, the EduDump.com ZDTA exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ZDTA dumps with Test Engine here:

<https://www.edudump.com/exams/Zscaler/ZDTA/premium/> (275 Q&As Dumps, **35%OFF**

Special Discount Code: **freecram**)

NEW QUESTION: 32

Which of the following enables the discovery of newly observed domains within three minutes of the domain coming online?

- A. IP Chicken
- B. MXToolbox
- C. Farsight Feed
- D. Dig

Answer: (SHOW ANSWER)

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

Farsight Feed is the correct choice because it supplies near-real-time passive DNS intelligence that helps Zscaler identify newly observed domains shortly after they appear. This supports protection against attacker infrastructure that may be registered or activated only minutes before phishing, command-and-control, malware delivery, or other malicious activity begins. Zscaler's Digital Transformation Administrator study material explains that Zscaler uses Farsight and other DNS sensor networks to detect domains as they emerge in DNS traffic, typically within minutes. IP Chicken is an external public-IP lookup utility, MXToolbox provides diagnostic and reputation tools, and Dig is a command-line DNS query utility; none is the Zscaler intelligence feed described in the question. Therefore, C is the only option that provides the required rapid newly observed domain discovery capability. See the official ZDTA study guide.

NEW QUESTION: 33

An investigation requires reviewing administrator entitlement changes from nine months ago to confirm suspected privilege escalation.

ZIdentity's default portal retention period has already elapsed.

Which approach helps preserve and access the required audit trail for governance and forensic analysis?

- A.** Export audit logs to CSV on a scheduled cadence and integrate supported audit streams with a SIEM through NSS or LSS to maintain an extended history
- B.** Rely on recent sign-on policy evaluations and extrapolate prior administrator actions from current configurations
- C.** Focus on bandwidth trends in Firewall Insights and infer administrative timelines from rule-utilization patterns
- D.** Depend on implicit caching in the Experience Center and query historical entries during off-peak hours

Answer: ([SHOW ANSWER](#))

Option A establishes an external record before portal retention expires. Zscaler's Log Streaming Service documentation states that LSS supports third-party SIEM integration and includes audit-log information among its supported content. The log-stream content reference also documents the audit-log format.

Administrators should export available records on a defined schedule and stream supported ZIA or ZPA administrative audit data to a SIEM with retention aligned to legal, compliance, and forensic requirements.

The SIEM then enables long-term correlation by administrator, action, timestamp, request ID, and affected object. Current configurations cannot reconstruct every historical change, and sign-on evaluations show authentication decisions rather than a complete entitlement-change history. Firewall Insights and ZDX Experience data describe traffic or performance; neither is an authoritative archive of administrator actions.

NEW QUESTION: 34

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: ([SHOW ANSWER](#))

Cross-Site Scripting injects malicious script into a trusted page so the victim's browser executes attacker-controlled code. Common XSS outcomes include session or cookie theft, unauthorized actions, and data exposure. Option C (Cookie Stealing) is correct because cookie stealing is a classic XSS impact.

Why the other options are incorrect:

- A). Spyware Callback: Spyware Callback is outbound C2 protection. It is not the browser/URL control being tested here.
- B). Anonymizers: Anonymizer controls restrict proxy/anonymity services. They do not represent the malicious-content category in this question.
- D). IRC Tunneling: IRC tunneling is a specific evasive communication method. The question's answer is the broader protection control being tested.

NEW QUESTION: 35

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: ([SHOW ANSWER](#))

Zscaler Cloud Firewall uses deep packet inspection to identify applications and protocols even when they attempt to use non-standard ports. This prevents evasive applications from bypassing policy simply by changing ports or disguising traffic. DPI then sends traffic to the appropriate enforcement engines. Option A (The Cloud Firewall includes Deep Packet Inspection, which detects protocol evasions and sends the traffic to the respective engines for inspection and handling) is correct because DPI is the mechanism that detects protocol evasion.

Why the other options are incorrect:

- B).** Zscaler Client Connector will prevent evasion on the endpoint in conjunction with the endpoint operating system's firewall: Zscaler Client Connector is the endpoint agent that steers traffic, authenticates users, reports posture, and supplies ZDX telemetry.
- 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: Relying on an on-premises firewall leaves evasive traffic outside Zscaler's cloud inspection decision. Zscaler Cloud Firewall uses DPI to identify protocol evasions itself.
- D).** The Cloud Firewall includes an IPS engine, which will detect the evasion techniques and will just block the transactions as it is invalid: IPS inspects traffic inline for exploit signatures and attack patterns, then blocks or resets offending sessions.

NEW QUESTION: 36

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: ([SHOW ANSWER](#))

Zscaler Access Control Services support Zero Trust by enforcing segmentation and conditional access instead of allowing broad network reach. Preventing lateral movement requires connecting users to specific applications and limiting what they can discover or reach beyond that entitlement. Option B (Access is granted without sharing the network between the originator and the destination application) is correct because segmentation and conditional access are the controls that reduce lateral-movement risk.

Why the other options are incorrect:

A). Trusted network criteria designate the locations of originators which can be trusted: Trusted Network detection decides whether the device is on a known corporate network using signals such as DNS servers, search domains, gateways, or hostname resolution.

C). Cloud firewall policies ensure that only authenticated users are allowed access to destination applications:

Zscaler Cloud Firewall enforces network-service and application rules for non-web and firewall-controlled traffic.

D). Connectivity between the originator and the destination application is over IPSec tunnels: IPS inspects traffic inline for exploit signatures and attack patterns, then blocks or resets offending sessions.

NEW QUESTION: 37

Which action should be taken during a regional policy-tuning effort that requires evidence of egress-control effectiveness by correlating rule-hit counts and application usage across locations under network-layer enforcement?

- A.** Review Data Discovery reports to visualize sensitive-data movement trends across channels
- B.** Check Administrator Audit Logs to evaluate configuration changes that might affect outcomes
- C.** Use Web Insights to compare browsing categories and threat actions across users and URLs
- D.** Open Firewall Insights to analyze rule-hit metrics, network-application usage, and bandwidth by location

Answer: D ([LEAVE A REPLY](#))

Firewall Insights is the correct analytical source because the requirement concerns network-layer egress enforcement. Zscaler's Firewall Insights columns reference includes the originating location and the network application associated with each session or aggregated session. Its filter reference allows administrators to narrow results by firewall or IPS action and other session attributes. The analyst can filter by region or location, matched rule and action, application, service, destination, and time range, then compare hit volume and transferred bytes before and after tuning. Data Discovery reports address sensitive-data exposure, not firewall enforcement. Administrator Audit Logs prove who changed configuration but do not measure traffic outcomes. Web Insights is appropriate for HTTP and HTTPS transactions, whereas the scenario explicitly requires network-layer application and firewall evidence. Firewall Insights therefore provides the required correlation.

NEW QUESTION: 38

A branch location must connect to Zscaler for web inspection. The underlay is trusted, the site requires a static egress IP mapped to the location, expected throughput is 700 Mbps, and high availability is not required.

Which tunnel approach and count meet these requirements with the least overhead?

- A.** Configure one IPSec tunnel to the regional Service Edge and declare the bandwidth expectation to match the site profile
- B.** Configure one GRE tunnel to a regional Service Edge and bind the location to a static IP to meet the throughput target
- C.** Provision two GRE tunnels to separate Service Edges and balance traffic through policy-based routing
- D.** Establish two IPSec peers with conservative IKE lifetimes to reduce rekey churn and configure the location's static IP

Answer: ([SHOW ANSWER](#))

One GRE tunnel is sufficient because the required 700 Mbps is below Zscaler's documented per-tunnel limit and the scenario does not require failover. Zscaler's GRE deployment best practices state that a GRE tunnel supports up to 1 Gbps when internal addresses are not behind NAT. The GRE self-provisioning guidance also explains that one static IP address can be mapped to a GRE tunnel. Because the underlay is trusted, GRE's lack of encryption is acceptable for this requirement and avoids IPSec encryption and rekey overhead. A single IPSec tunnel is unsuitable for 700 Mbps because Zscaler documents a lower per-public-source-IP limit for IPSec. Two tunnels add unnecessary configuration and routing complexity when high availability is explicitly excluded. Capacity, MTU, routing, and Service Edge reachability should still be validated before production use.

NEW QUESTION: 39

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: ([SHOW ANSWER](#))

Device attributes in a SAML assertion become policy context inside the Zero Trust Exchange. Zscaler consumes those attributes as part of identity and session context so downstream ZIA or ZPA policies can evaluate device state during access decisions. Option D (Zero Trust Exchange) is correct because the Zero Trust Exchange is the policy-enforcement fabric that uses those attributes.

Why the other options are incorrect:

- A). Enforcement node: An enforcement node applies decisions to traffic. The attributes must first be consumed and normalized by the Zero Trust Exchange policy context.

B). Zscaler SAML SP: SAML provides browser-based federation by carrying signed assertions from the identity provider to the service provider.

C). Mobile Admin Portal: Mobile Admin Portal/Client Connector administration is for endpoint-agent configuration, not the identity-policy component in the stem.

NEW QUESTION: 40

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: ([SHOW ANSWER](#))

Client Connector automatically checks for software updates on a recurring schedule so endpoint agents remain current without manual user action. The tested default software-update interval is two hours. Option C (Every 2 hours) is correct because the automatic software-update check occurs every two hours.

Why the other options are incorrect:

- A). Every 6 hours: Six hours would delay client software update checks beyond the default cadence. Zscaler Client Connector checks the software update policy every two hours.
- B). Every 12 hours: Twelve hours is far too slow for the default software update policy check. The default interval is two hours.
- D). Every 24 hours: Twenty-four hours would mean only a daily update-policy check. ZCC checks software update policy much more frequently: every two hours.

NEW QUESTION: 41

Audit logs show configuration changes performed by members of a group outside its intended administrative area.

Which step reduces this exposure while preserving required functionality?

- A. Adjust department classifications to redefine reporting lines for the group
- B. Switch to just-in-time provisioning only so that attributes are reapplied during every session
- C. Revise the group's administrative entitlements and role assignments to constrain its scope according to least privilege
- D. Relax sign-on policies to reduce failed authentication events across locations

Answer: C ([LEAVE A REPLY](#))

The audit evidence shows excessive authorization, so the correction must be made to the group's administrative permissions and scope. Zscaler's Authentication Service role documentation explains that role-based administration assigns users or groups defined roles and permissions that control their level of administrative access. Zscaler also provides administrative entitlement management for assigning groups the required administrator roles. The administrator should identify the unauthorized actions in the audit logs, remove unneeded entitlements, restrict the role or tenant scope, and retest legitimate tasks. Department labels do not enforce administrative

permissions. JIT provisioning can refresh identity data but does not correct an overprivileged role. Relaxing sign-on policy would reduce authentication security and has no connection to configuration authorization. Option C preserves necessary duties while removing access outside the group's intended administrative area.

NEW QUESTION: 42

Which Zscaler feature detects whether an intruder is accessing your internal resources?

- A.** SandBox
- B.** SSL Decryption Bypass
- C.** Browser Isolation
- D.** Deception

Answer: ([SHOW ANSWER](#))

Cloud Browser Isolation protects users by rendering risky web content in a remote browser environment instead of on the endpoint. URL Filtering can use Isolate as an action, so users may still access selected untrusted sites while scripts, active content, and browser-exploit risk remain separated from the device.

Option D (Deception) is correct because isolation is an enforceable URL Filtering action, not a separate manual workaround.

Why the other options are incorrect:

- A). SandBox: Cloud Sandbox detonates and observes suspicious files to identify unknown or advanced malware behavior.
- B). SSL Decryption Bypass: SSL/TLS bypass tells the proxy to pass encrypted traffic without decrypting it for content inspection.
- C). Browser Isolation: Browser Isolation renders web content remotely so active content never executes directly on the endpoint.

NEW QUESTION: 43

Live logs show a global DLP rule that blocks uploads of regulated financial data and a departmental override that allows uploads for Finance when device posture is compliant. A Finance user on a compliant device successfully uploads a spreadsheet containing regulated data to a generic file-sharing application, despite expectations that the upload would be blocked. The departmental allow rule appears before the global block rule.

Which conclusion and next step best address the issue?

- A.** Escalate to the data-protection team to adjust rule precedence so that the global block evaluates before the departmental allow and prevents the upload
- B.** Instruct the network team to increase the default URL-risk threshold, anticipating fewer permitted uploads through stricter categorization
- C.** Reduce OCR sensitivity for spreadsheet inspection to limit misclassifications and reduce false negatives in content analysis
- D.** Revise Advanced Threat Protection sensitivity to reduce permissive outcomes on newly observed destinations and defer DLP rule changes

Answer: ([SHOW ANSWER](#))

The successful upload is explained by DLP rule precedence, not URL reputation or threat sensitivity. Zscaler documents that, by default, inline DLP rules are evaluated according to rule order and evaluation stops at the first match. The Finance user satisfies the earlier departmental allow rule, so the later global block is not reached. The data-protection owner should narrow or reposition the exception so regulated-data blocking takes precedence for generic file-sharing destinations. If the organization enables Evaluate All Rules, it must instead validate the configured action-selection behavior and matching engines because evaluation differs from default first-match mode. URL-risk thresholds and Advanced Threat Protection govern destination or threat risk, not sensitive-content authorization. Lowering OCR sensitivity would weaken content detection and could create additional data-loss gaps. Option A directly corrects the policy condition shown in the logs.

NEW QUESTION: 44

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: ([SHOW ANSWER](#))

ZPA grants access only after the request satisfies the authorization and security conditions in policy. This is core Zero Trust behavior: identity is verified, context is checked, device posture may be evaluated, and least-privilege rules determine whether a segmented private app is reachable. Option A (After passing criteria checks related to authorization and security) is correct because access is conditional on passing the defined criteria, not on merely initiating a connection.

Why the other options are incorrect:

- B).** Immediately upon connection request for best performance: Immediate access would skip the Zero Trust decision. ZPA first checks identity, context, posture, and policy before creating the private-app connection.
- C).** After a short delay of a random number of seconds: Random delay is not a security control in ZPA. Access is granted or denied predictably after the rule conditions are evaluated.
- D).** After verifying the user password inside of private application: The private application may still have its own login, but ZPA conditional access is decided before the user reaches that app. ZPA is the access broker, not the application password checker.

NEW QUESTION: 45

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.

Answer: D ([LEAVE A REPLY](#))

In ZPA, Server Groups define back-end server reachability and are associated with App Connector Groups that can resolve and check those servers. Dynamic Server Discovery lets the mapped connector groups discover or resolve application servers and perform health checks before traffic is steered. Option D (Server Groups are configured for Dynamic Server Discovery so that mapped Connector Groups can DNS resolve and make health checks toward the application) is correct because Server Groups provide the discovery/health-check relationship to the mapped Connector Groups.

Why the other options are incorrect:

A). Server Groups are configured for Dynamic Server Discovery so that mapped Connector Groups can then DNS resolve individual application Segment Groups: A Server Group groups application servers and maps them to App Connector Groups that can reach those servers.

B). Connector Groups are configured for Dynamic Server Discovery so that mapped Server Groups can DNS resolve and advertise the applications: A Server Group groups application servers and maps them to App Connector Groups that can reach those servers.

C). Connector Groups are configured for Dynamic Server Discovery so that ZPA can steer traffic through the appropriate Server Group: A Server Group groups application servers and maps them to App Connector Groups that can reach those servers.

NEW QUESTION: 46

A regional office reports persistent throttling of a critical SaaS application during business hours. The Bandwidth Control dashboard shows the application assigned to a class with a narrow maximum, while rule-hit counts indicate that non-critical streaming traffic is receiving excessive bandwidth.

Which action should the network team take to improve performance?

A. Add a parallel rule for the critical application in the same class to increase match frequency despite the existing caps

B. Broaden minimum bandwidth globally, accepting reduced headroom for all locations to offset localized congestion

C. Stream firewall logs to the SIEM and defer policy updates until multi-source correlation identifies external bottlenecks

D. Refactor the bandwidth-class definitions and rule order to increase the critical application's allocation and restrict non-critical streaming, then validate the change in Firewall Insights

Answer: ([SHOW ANSWER](#))

Option D directly corrects both configuration problems shown by the evidence: the critical SaaS application has an overly restrictive class maximum, and lower-priority streaming traffic has excessive allocation. ZIA Bandwidth Control uses bandwidth classes and policy rules to allocate or limit traffic, so the administrator should revise the relevant class values and ensure that rule order produces the intended match. Zscaler's Bandwidth Control overview and bandwidth-rule configuration guidance support managing allocations through classes and ordered rules. Firewall Insights can then confirm application usage and policy effects. A duplicate rule cannot bypass the existing class cap. A global increase wastes capacity and may worsen contention elsewhere. Sending logs to a SIEM may aid investigation, but delaying an evidence-supported correction leaves the known throttling condition unresolved.

Valid ZDTA Dumps shared by EduDump.com for Helping Passing ZDTA Exam!

EduDump.com now offer the **newest ZDTA exam dumps**, the EduDump.com ZDTA exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ZDTA dumps with Test Engine here:

<https://www.edudump.com/exams/Zscaler/ZDTA/premium/> (275 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 47

A team needs to validate who changed an entitlement and whether the change succeeded, and then correlate the activity with broader events.

Which audit source best supports this review before adding SIEM context?

- A.** DLP event dashboards, because data-movement visualizations can uncover configuration edits through exposure trend shifts
- B.** Firewall Insights, because network-layer telemetry can expose configuration changes through connection-state deviations
- C.** Web Insights, because application traffic views can infer administrative behavior through session lineage and path analysis
- D.** ZIdentity or Administrator Management audit logs, because they record administrator actions with the actor, timestamp, target, and outcome for direct attribution

Answer: (SHOW ANSWER)

Option D provides direct administrative evidence rather than an inference from user traffic. Zscaler's ZPA Audit Logs documentation states that audit logs display administrator sign-in and sign-out attempts, actions, request IDs, and completed configuration changes. Those records establish who performed an entitlement-related action, when it occurred, and what operation was attempted or completed. The relevant audit entry should be validated first and then correlated with identity, endpoint, and security events in the SIEM using its timestamp and request or transaction identifiers. DLP dashboards describe sensitive-data events; Firewall Insights describes network sessions and policy activity; and Web Insights describes web transactions.

None is authoritative for attributing an administrator's configuration change. Audit logs therefore supply the defensible source record before broader SIEM correlation.

NEW QUESTION: 48

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

Answer: ([SHOW ANSWER](#))

Identity Threat Detection and Response focuses on identity risk, particularly in directory environments such as Active Directory. To evaluate AD objects, relationships, permissions, and risky identity configurations, ITDR needs directory-level data rather than raw packet captures or firewall summaries. Option B (Reduces identity related risks) is correct because LDAP queries are the standard mechanism for collecting structured AD domain information for identity-risk analysis.

Why the other options are incorrect:

- A). Prevents Patient Zero Infections: Patient Zero prevention is malware-first prevention. ITDR reduces identity risk by finding credential, privilege, and directory exposures.
- C). Prevents connections to Embargoed Countries: Embargoed-country blocking is geo/access policy. ITDR is focused on identity threats, not destination-country filtering.
- D). Blocks malicious traffic by dropping packets: Dropping packets is firewall/IPS behavior. ITDR analyzes identities and permissions rather than acting as a packet filter.

NEW QUESTION: 49

A platform team deploys Bandwidth Control and firewall policy changes through an API. After a large rollout, users report sporadic application slowdowns, yet the monitoring team finds gaps in telemetry for the same time windows.

Which action best prevents these performance issues from persisting and going undetected in similar rollouts?

- A.** Add an implementation step that validates monitoring subscriptions and exports ZDX and Firewall Insights baselines before applying policy changes through APIs
- B.** Aggregate logs monthly and perform retrospective correlation to avoid noisy short-term fluctuations in metrics
- C.** Increase API client-token lifetimes to reduce HTTP 401 errors and stabilize automation during policy pushes
- D.** Restrict automation runs to weekly windows to minimize configuration changes that may obscure trend lines

Answer: ([SHOW ANSWER](#))

Option A adds the missing observability control before a high-impact automated change.

Validating monitoring subscriptions helps ensure that telemetry will be collected during the rollout,

while exporting pre- change ZDX and Firewall Insights baselines creates a reference for detecting latency, loss, application, and policy-behavior regressions. Zscaler's ZDX Reference Architecture recommends controlled deployment and validation, and the Internet and SaaS performance troubleshooting runbook uses ZDX and Firewall Insights as complementary evidence sources. Monthly aggregation is too delayed for rollout protection. Longer API- token lifetimes address authentication continuity, not missing monitoring data or application performance. Running automation weekly merely reduces deployment frequency; it does not prove telemetry coverage or provide a reliable before-and-after comparison for each policy change.

NEW QUESTION: 50

Which options must be selected when configuring Zscaler Client Connector for Strict Enforcement?

- A.** cloudName and policyToken
- B.** userDomain and deviceToken
- C.** cloudName and deviceToken
- D.** userDomain and policyToken

Answer: A ([LEAVE A REPLY](#))

Strict Enforcement requires the installer to know both which Zscaler cloud to enroll against and which policy token authorizes the enforcement configuration. The cloudName parameter directs the client to the correct cloud, while policyToken applies the required strict-enforcement policy during enrollment. Option A (cloudName and policyToken) is correct because those two options are the required installer inputs.

Why the other options are incorrect:

- B). userDomain and deviceToken: userDomain tells Client Connector the user login domain so it can route enrollment toward the right IdP.
- C). cloudName and deviceToken: cloudName tells the installer which Zscaler cloud or tenant environment the client should use.
- D). userDomain and policyToken: userDomain tells Client Connector the user login domain so it can route enrollment toward the right IdP.

NEW QUESTION: 51

A Cloud Sandbox detonation shows a document beaconing through obfuscated scripts and spawning child processes that attempt network calls to newly registered domains. The desired outcome is to prevent users from downloading or accessing similar suspicious files across web and SaaS channels.

What action should be taken next?

- A.** Apply a Sandbox policy that quarantines the document type across all applicable channels above the existing Sandbox policy rule
- B.** Shift scanning to out-of-band CASB-only workflows so that analysis occurs after content is stored
- C.** Route detections to a manual review queue and postpone policy changes until more analyst capacity is available

D. Lower Sandbox sensitivity to reduce alert volume and defer enforcement until trend data is gathered

Answer: ([SHOW ANSWER](#))

The observed beaconing, script obfuscation, child-process creation, and calls to newly registered domains justify preventive enforcement. In a ZIA Sandbox rule, Quarantine holds an unknown file while analysis is performed, as documented in Configuring the Sandbox Policy. A more specific rule for the affected document type and required users, locations, or destinations should be placed above a broader existing rule so it is evaluated first. Applicable web and SaaS delivery paths should be included to avoid a channel gap. If analysis determines the file is safe, the configured workflow can release it; a malicious verdict prevents delivery and supports follow-up investigation. Out-of-band-only scanning occurs after storage and does not provide equivalent inline prevention. Manual review delays containment, and lowering sensitivity reduces protection despite strong malicious behavior. Option A therefore prevents another patient-zero download while retaining controlled analysis.

NEW QUESTION: 52

Is SCIM mandatory for ZIA?

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

Answer: ([SHOW ANSWER](#))

SCIM is useful for automated provisioning, group synchronization, and lifecycle management, but it is not mandatory for ZIA authentication. ZIA can authenticate users through SAML and other supported identity methods even if SCIM is not deployed. Option A (No) is correct because SCIM is optional for ZIA, not required.

Why the other options are incorrect:

- B). Depends: Depends would only be acceptable if the question were asking for design preference. The direct fact tested here is that SCIM is not mandatory for ZIA.
- C). Yes: Yes would make SCIM a hard requirement. ZIA can authenticate and apply policy without mandatory SCIM provisioning.
- D). Maybe: Maybe is not a platform behavior. SCIM is optional for ZIA, even though it is useful for automated lifecycle management.

NEW QUESTION: 53

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

Answer: (SHOW ANSWER)

Workflow Automation is used to notify users or teams when a DLP-related workflow needs attention. For end-user notification, enterprise collaboration tools such as Microsoft Teams and Slack are practical because they keep the message inside a controlled business channel. Option A (Notifications in MS Teams / Slack) is correct because Teams and Slack notifications are the supported user-notification path in this scenario.

Why the other options are incorrect:

B). SMS text message: SMS is a generic notification channel. Zscaler Workflow Automation for this use case sends collaboration notifications through tools like Teams or Slack.

C). Automated phone call: Automated phone calls are not the normal DLP workflow-notification method in this Zscaler scenario. The supported peer-collaboration channels are Teams and Slack.

D). Twitter post with custom hashtag: A Twitter/X post would be public and inappropriate for a DLP event.

Zscaler uses controlled enterprise notification channels, not social posting.

NEW QUESTION: 54

What is a Landmine in Deception?

A. Agentless plug-in installed on endpoints, such as desktops or laptops on a network. These plug-ins deploy decoy credentials, files, processes, and lures to other decoys at endpoints.

B. Software agent installed on a centralized server in datacenter or in cloud. The agents running in the server deploy decoy credentials, files, processes, and lures to other decoys at endpoints.

C. Software agent installed on endpoints, such as desktops or laptops on a network. These agents deploy decoy credentials, files, processes, and lures to other decoys at endpoints.

D. Agentless plug-in installed on endpoints, such as desktops or laptops on a network. These plug-ins auto rotate decoy credentials, files, processes, and lures to other decoys at endpoints.

Answer: (SHOW ANSWER)

A Deception Landmine is endpoint software that plants decoy artifacts such as fake credentials, files, processes, or lures. Those artifacts are designed to attract attackers who are moving laterally or harvesting credentials, causing high-fidelity alerts when touched. Option C (Software agent installed on endpoints, such as desktops or laptops on a network. These agents deploy decoy credentials, files, processes, and lures to other decoys at endpoints) is correct because a Landmine is an endpoint agent that deploys deception lures from the endpoint.

Why the other options are incorrect:

A). Agentless plug-in installed on endpoints, such as desktops or laptops on a network. These plug-ins deploy decoy credentials, files, processes, and lures to other decoys at endpoints: Deception uses decoys, fake credentials, lures, and traps to expose intruders who are exploring the environment.

B). Software agent installed on a centralized server in datacenter or in cloud. The agents running in the server deploy decoy credentials, files, processes, and lures to other decoys at endpoints:

Deception uses decoys, fake credentials, lures, and traps to expose intruders who are exploring the environment.

D). Agentless plug-in installed on endpoints, such as desktops or laptops on a network. These plug-ins auto rotates decoy credentials, files, processes, and lures to other decoys at endpoints: Deception uses decoys, fake credentials, lures, and traps to expose intruders who are exploring the environment.

NEW QUESTION: 55

Which proprietary technology does Zscaler use to calculate risk attributes dynamically for websites?

- A. Third-Party Sandbox
- B. Zscaler PageRisk
- C. Browser Isolation Feedback Form
- D. Deception Controller

Answer: (SHOW ANSWER)

Zscaler PageRisk, specifically the Page Risk Index, is the proprietary scoring capability used in ZIA to evaluate the risk of web pages dynamically. Instead of relying only on static URL blocklists, PageRisk uses a multi-data algorithm that considers page content and domain characteristics. Page-content signals include risky scripts, suspicious iFrames, XSS indicators, vulnerable controls, and other active content. Domain signals include reputation, hosting location, age, and relationships to risky top-level domains. The verified answer is Option B (Zscaler PageRisk) because PageRisk is the Zscaler technology used for real-time website risk scoring.

Why the other options are incorrect:

A). Third-Party Sandbox: A sandbox detonates files to observe malicious behavior. PageRisk is a web-page

/domain scoring engine, and Zscaler uses native sandboxing rather than a third-party PageRisk service.

C). Browser Isolation Feedback Form: Browser Isolation renders risky pages remotely to protect the endpoint.

A feedback form would collect input; it would not calculate real-time web risk.

D). Deception Controller: The Deception controller manages decoys, lures, and honeytokens for intruder detection. It is about lateral-movement detection, not public website scoring.

NEW QUESTION: 56

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.

Answer: (SHOW ANSWER)

ZDX includes endpoint and network-path visibility, including Wi-Fi health indicators. A poor signal can appear in device health telemetry and in Cloud Path Probe context, allowing the administrator to separate a local wireless problem from Zscaler, ISP, or application issues. Option 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) is correct because Wi-Fi signal degradation is visible through ZDX telemetry.

Why the other options are incorrect:

- A). Yes, the Wi-Fi hop latency is shown on a cloud path probe: Wi-Fi signal and Wi-Fi hop latency are endpoint/local-network indicators used by ZDX troubleshooting.
- B). Yes. but the current Wi-Fi signal strength is only displayed when doing a deep trace: Deep Trace is a detailed diagnostic capture; it is useful, but slower and more manual than Y-Engine root-cause analysis.
- C). No, ZDX only works on hardwired devices: ZDX works on supported endpoints running Client Connector, including devices on Wi-Fi. It can expose Wi-Fi signal problems instead of requiring wired-only access.

NEW QUESTION: 57

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: (SHOW ANSWER)

Cloud Browser Isolation protects users by rendering risky web content in a remote browser environment instead of on the endpoint. URL Filtering can use Isolate as an action, so users may still access selected untrusted sites while scripts, active content, and browser-exploit risk remain separated from the device.

Option A (Browser Isolation) is correct because isolation is an enforceable URL Filtering action, not a separate manual workaround.

Why the other options are incorrect:

- B). App Connector: An App Connector brokers outbound connectivity to private apps. It does not make untrusted public URLs safe for user browsing.
- C). Zscaler Private Access: ZPA secures private applications. The scenario is public/untrusted web browsing, which is handled by Browser Isolation through ZIA policy.
- D). Zscaler Client Connector: Zscaler Client Connector is the endpoint agent that steers traffic, authenticates users, reports posture, and supplies ZDX telemetry.

NEW QUESTION: 58

What is the purpose of a Microtunnel (M-Tunnel) in Zscaler?

- A. To provide an end-to-end communication channel between ZCC clients
- B. To provide an end-to-end communication channel to Microsoft Applications such as M365
- C. To create an end-to-end communication channel to Azure AD for authentication
- D. To create an end-to-end communication channel to internal applications

Answer: D ([LEAVE A REPLY](#))

A ZPA microtunnel is the per-application communication channel created after the user is authenticated and authorized. It carries traffic from the user side through the Zscaler service edge to the App Connector path for the internal application. Option D (To create an end-to-end communication channel to internal applications) is correct because the M-Tunnel is built for private application communication, not endpoint-to-endpoint or IdP connectivity.

Why the other options are incorrect:

- A). To provide an end-to-end communication channel between ZCC clients: ZCC-to-ZCC communication would be peer endpoint connectivity. A ZPA microtunnel is created from the user side toward a specific internal application.
- B). To provide an end-to-end communication channel to Microsoft Applications such as M365: Microsoft 365 optimization uses local breakout, DNS locality, and inspection bypass where Microsoft recommends it for performance.
- C). To create an end-to-end communication channel to Azure AD for authentication: Azure AD communication is part of authentication. The microtunnel carries private-application traffic after access is authorized.

NEW QUESTION: 59

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: ([SHOW ANSWER](#)**)**

Microsoft Information Protection labels imported into ZIA are used as criteria in DLP policy enforcement. A custom DLP policy can inspect data in motion and take actions based on the sensitivity labels attached to documents. Option D (Creating a custom DLP Policy) is correct because MIP labels are consumed in DLP policy logic, not in PAC, file type, or posture policies.

Why the other options are incorrect:

- A). Creating a custom DLP Dictionary: A custom DLP Dictionary defines match patterns. Imported MIP labels are used in DLP policy conditions/actions, not turned into a dictionary.
- B). Creating a SaaS Security Posture Control Policy: SSPM checks SaaS tenant configuration, risky settings, and compliance posture.
- C). Creating a File Type Control Policy: File Type Control classifies and restricts uploads or downloads by file type, regardless of filename tricks.

NEW QUESTION: 60

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: ([SHOW ANSWER](#))

A URL Filtering Caution action is designed for web-style requests where the user can be warned before proceeding. The supported request methods tested here are Connect, GET, and HEAD, which align with browser-driven web access and HTTPS tunnel establishment. Option A (Connect, Get, Head) is correct because those methods are valid for the Caution action.

Why the other options are incorrect:

- B). Options, Delete, Put: OPTIONS, DELETE, and PUT are HTTP methods, but the canonical REST basics in the guide include GET, POST, PUT, and DELETE.
- C). Get, Delete, Trace: TRACE is an HTTP diagnostic method and is not part of the standard REST method set emphasized for Zscaler automation.
- D). Connect, Post, Put: CONNECT is proxy tunneling behavior. REST API basics focus on resource methods such as GET, POST, PUT, and DELETE.

NEW QUESTION: 61

Which three levels of inspection are used by Zscaler for File Type Identification?

- A. Mime type, file extension and file size
- B. File extension, content type and file size
- C. Magic bytes, mime type and file extension
- D. Magic bytes, mime type and MS Office version

Answer: ([SHOW ANSWER](#))

Zscaler File Type Identification uses more than a file extension because attackers can rename files to bypass simple checks. The inspection process evaluates magic bytes, MIME type, and file extension to classify files more accurately before applying File Type Control policy. Option C (Magic bytes, mime type and file extension) is correct because those are the three inspection levels tested here.

Why the other options are incorrect:

- A). Mime type, file extension and file size: MIME type is metadata declaring the content type of a transferred object.
- B). File extension, content type and file size: File extension is the visible suffix such as .exe or .docx; it is useful but easy for attackers to rename.
- D). Magic bytes, mime type and MS Office version: Magic bytes are header values inside a file that reveal the real file type even if the extension is changed.

Valid ZDTA Dumps shared by EduDump.com for Helping Passing ZDTA Exam!

EduDump.com now offer the **newest ZDTA exam dumps**, the EduDump.com ZDTA exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com ZDTA dumps with Test Engine here:

<https://www.edudump.com/exams/Zscaler/ZDTA/premium/> (275 Q&As Dumps, **35%OFF**)

Special Discount Code: **freecram**)

NEW QUESTION: 62

A device connects to the Zero Trust Exchange with missing antivirus telemetry and an unverified client certificate in its posture profile.

Assuming Leading Practice for posture-driven enforcement are implemented, what is the outcome for the session?

- A.** Route to the nearest service edge and record a posture exception in logs
- B.** Apply an isolation policy that constrains interaction until posture is compliant
- C.** Treat the session as trusted because the network context is corporate Wi-Fi
- D.** Defer the decision to the identity provider due to incomplete posture telemetry

Answer: B ([LEAVE A REPLY](#))

Answer B is correct. Missing antivirus telemetry and an unverified client certificate mean the device does not satisfy the required posture profile. Under the stated leading-practice design, the session should not receive ordinary application access. A policy can instead direct the user to an isolated browser experience, limiting interaction and preventing sensitive data from reaching the endpoint until the posture requirements are met.

ZPA Access Policies can use posture profiles as criteria, while Isolation Policy provides controlled access to eligible private web applications. Corporate Wi-Fi is only network context and must not override failed device verification. The identity provider establishes user identity, but it does not resolve missing endpoint security evidence. Administrators should also log the failed posture conditions for remediation and investigation. See Zscaler's Isolation Policy overview and Access Policy configuration.

NEW QUESTION: 63

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: ([SHOW ANSWER](#)**)**

Zscaler SaaS Security Posture Management evaluates supported SaaS platforms for risky configurations, posture gaps, and compliance issues. Google Workspace is one of the supported SaaS environments for posture assessment, whereas storage or collaboration tools in the other

choices do not match this SSPM support item. Option D (Google Workspace) is correct because Google Workspace is the supported SaaS platform in this question.

Why the other options are incorrect:

A). Amazon S3: Amazon S3 is cloud object storage, not the SaaS collaboration suite named by the tested SSPM support item.

B). Webex Teams: Webex Teams is a collaboration app. The question's intended application/control is not Webex Teams.

C). Dropbox: Dropbox is cloud storage. It is a common SaaS destination, but it is not the application identified by the scenario's correct answer.

NEW QUESTION: 64

An organization has more than one ZIA instance, each on different clouds. The organization is using the same login domain for both and upon login users are given this menu in ZCC asking which cloud they would like to join. What steps could an Administrator take to avoid having this menu appear?

A. Customize an MSI version of the ZCC file specifying the USERDOMAIN variable.

B. Customize an MSI version of the ZCC file specifying the CLOUDNAME variable.

C. Federate the login domain between two different IDP instances.

D. Create only one SAML integration with the desired ZIA instance.

Answer: ([SHOW ANSWER](#))

When multiple ZIA tenants or clouds share the same login domain, Client Connector may display a cloud- selection prompt. The CLOUDNAME installer parameter pins the client to the intended Zscaler cloud so users are not asked to choose during enrollment or login. Option B (Customize an MSI version of the ZCC file specifying the CLOUDNAME variable) is correct because CLOUDNAME removes the cloud-selection ambiguity.

Why the other options are incorrect:

A). Customize an MSI version of the ZCC file specifying the USERDOMAIN variable: userDomain tells Client Connector the user login domain so it can route enrollment toward the right IdP.

C). Federate the login domain between two different IDP instances: Federating the login domain between IdPs changes authentication design. It will not stop Client Connector from showing a cloud-selection menu when the tenant cloud is ambiguous.

D). Create only one SAML integration with the desired ZIA instance: SAML provides browser-based federation by carrying signed assertions from the identity provider to the service provider.

NEW QUESTION: 65

Cloud Sandbox detonations begin returning indicators of compromise associated with TrickBot infrastructure, including domains and IP addresses. The SOC wants consistent enforcement in ZIA with less manual effort.

Which operational approach best fits this goal?

A. Perform daily manual updates to a URL blocklist and a separate firewall address group for each new indicator, deferring changes during peak hours

- B.** Switch IPS to detect-only mode to gather more evidence and postpone blocking until campaign indicators stabilize across multiple users
- C.** Increase Advanced Threat Protection risk sensitivity and rely on page-risk analysis to identify newly observed destinations
- D.** Use a SOAR workflow with Zscaler APIs to add domains to a custom URL category and IP addresses to a firewall destination group, with block policies applied automatically

Answer: D ([LEAVE A REPLY](#))

Option D converts verified Sandbox intelligence into repeatable enforcement. Zscaler's ZIA API documentation includes operations for updating custom URL categories with URLs or IP addresses and managing Firewall Filtering resources. Zscaler's Splunk integration guide also documents a SOAR playbook that correlates malicious IPs and domains with ZIA logs, checks the existing denylist, and updates it through an API when needed. The workflow should validate indicator format, avoid duplicate entries, activate the relevant URL and firewall policies, record changes, and support rollback. Manual updates are slower and inconsistent. Detect-only IPS deliberately postpones containment, while increasing a general risk setting does not guarantee that the known TrickBot indicators are blocked. Automated, audited API updates provide the precise and scalable response requested.

NEW QUESTION: 66

A team begins using domains that were dormant for months and recently revived. TLS inspection is enabled, but some teams added URL exceptions that bypass malware inspection.

Which action should a ZIA administrator take to prevent callbacks while minimizing disruption?

- A.** Enable Browser Isolation for all sites flagged as recently active and let sessions render in isolation to reduce potential impact
- B.** Depend on Advanced Threat Protection risk scoring by raising the risk threshold so borderline pages are treated as unsafe and blocked across categories
- C.** Remove URL scanning exceptions for the affected teams, enforce a block policy targeting the Newly Revived Domains category, and configure DNS security to deny resolution for those hostnames
- D.** Apply detect-only IPS mode to observe behavior, then plan a gradual transition to blocking after signatures show sustained activity

Answer: ([SHOW ANSWER](#)**)**

Option C closes both identified gaps. The URL exceptions currently let traffic avoid malware inspection, so they should be removed or narrowed. Zscaler added Newly Revived Domains to the Security URL super- category specifically for domains reactivated after a period of inactivity. A scoped URL Filtering block can stop web access to that category. Zscaler's predefined DNS Control rule guidance also identifies newly revived domains among the threats that DNS Control can block, preventing resolution before a callback is established. Isolation still permits a controlled browsing session and is not the strongest response to suspected command-and-control callbacks. Raising a generic risk threshold is less precise, while detect-only IPS records activity

without preventing it. Layered URL and DNS enforcement provides targeted protection with less disruption than a broad block.

NEW QUESTION: 67

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: ([SHOW ANSWER](#))

In ZPA, Server Groups define which App Connector Groups can reach the application servers behind an Application Segment. They are part of the mapping that lets ZPA choose the correct outbound connector path for private application traffic. Option C (Maps App Connector Groups to Application Segments) is correct because Server Groups map App Connector Groups to Application Segments for reachability and steering.

Why the other options are incorrect:

- A). Maps FQDNs to IP Addresses: DNS resolves names to IP addresses; it is a support service, not an access protocol or scoring engine by itself.
- B). Maps Applications to FQDNs: DNS resolves names to IP addresses; it is a support service, not an access protocol or scoring engine by itself.
- D). Maps Applications to Application Groups: Mapping applications to application groups is a policy- organization task. Server Groups specifically map reachable application servers to App Connector Groups.

NEW QUESTION: 68

What is a seed in Asset Discovery within External Attack Surface Management?

- A.** A legitimate organizational asset, such as a known domain, IP address, or IP block, that serves as the starting point for discovery.
- B.** A legitimate asset used to discover sensitive data and identify users accessing sanctioned or unsanctioned applications.
- C.** A legitimate asset that allows users to access websites that are not mission-critical or business-critical.
- D.** A legitimate decoy asset that triggers notifications and Deception actions when contacted by an attacker.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

In Zscaler External Attack Surface Management, a seed is a known, legitimate asset supplied by the organization as the starting point for discovery, making A correct. Seeds can be domains, public IP addresses, or IP blocks associated with the organization. Zscaler EASM analyzes relationships connected to these seeds to identify additional internet-facing assets and build a

more complete external attack-surface inventory. A seed is not a Data Discovery object for tracking sensitive information or SaaS usage, and it does not grant users access to noncritical websites. It is also not a decoy used by Zscaler Deception to detect attacker interaction. The official Asset Discovery documentation defines a seed as a legitimate organizational asset that initiates the discovery process, directly matching option A.

NEW QUESTION: 69

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: (SHOW ANSWER)

Legacy firewalls introduce performance risk because they were designed around centralized perimeter enforcement and hardware capacity limits. Cloud and remote-work traffic creates encrypted, high-volume flows that can overwhelm appliance-based inspection and force inefficient backhauling. Option A (Performance issues) is correct because performance degradation is a real business risk of legacy firewall architecture.

Why the other options are incorrect:

- B). Reduced management: Reduced management would be an operational benefit, not a business risk introduced by legacy firewalls.
- C). Low costs: Low cost is a benefit claim, while legacy firewall estates usually add hardware, scaling, and maintenance cost.
- D). Low licensing support: Licensing support is a commercial concern, not the main architectural risk tested in the legacy-firewall question.

NEW QUESTION: 70

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: (SHOW ANSWER)

SAML authenticates the user at login time, but efficient user provisioning needs automated lifecycle mechanisms. SCIM synchronizes users, groups, and attributes from the IdP, while SAML auto-provisioning

/JIT can create users dynamically during successful authentication. Option D (SCIM and SAML Autoprovisioning) is correct because SCIM and SAML auto-provisioning are the efficient provisioning methods.

Why the other options are incorrect:

- A). Hosted User Database and Directory Server Synchronization: A hosted user database is manual or local account storage; it does not automate lifecycle changes as cleanly as SCIM/JIT.
- B). SAML and Hosted User Database: SAML can create users at sign-in with JIT, but by itself it is an authentication assertion, not continuous lifecycle synchronization like SCIM.
- C). SCIM and Directory Server Synchronization: SCIM provisions and synchronizes users, groups, and attributes between an identity provider and Zscaler.

NEW QUESTION: 71

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: (SHOW ANSWER)

Identity Threat Detection and Response focuses on identity risk, particularly in directory environments such as Active Directory. To evaluate AD objects, relationships, permissions, and risky identity configurations, ITDR needs directory-level data rather than raw packet captures or firewall summaries. Option B (Running LDAP queries) is correct because LDAP queries are the standard mechanism for collecting structured AD domain information for identity-risk analysis.

Why the other options are incorrect:

- A). Scanning network ports: Port scanning discovers open TCP/UDP services on hosts. ITDR needs AD identity data, so it queries the directory instead of scanning network sockets.
- C). Analyzing firewall logs: Firewall logs show network sessions and policy outcomes. They do not expose AD object relationships, permissions, or identity hygiene the way LDAP directory queries do.
- D). Packet sniffing: Packet sniffing captures traffic on the wire. ITDR is not passively sniffing packets here; it gathers structured domain information from Active Directory.

NEW QUESTION: 72

A threat actor's command-and-control infrastructure uses hard-coded IP addresses and several domains resolved through DNS. An organization wants Zscaler to block callback attempts with minimal dependence on endpoint agents and to enforce the decision consistently for roaming users.

Which configuration best aligns with ZIA policy enforcement and the zero-trust model?

- A.** Enable Browser Isolation for the suspected destinations so sessions are rendered remotely even when callbacks reach the external hosts
- B.** Add the domains to a URL-category override and depend on TLS inspection to identify the traffic after connection
- C.** Create a high-risk URL Filtering rule that reduces the Advanced Threat Protection risk threshold and relies on page scoring to suppress suspicious domains

D. Create a Cloud Firewall destination group containing the indicator IP addresses and apply a high- priority Drop rule, while adding the domains to a globally blocked custom URL category

Answer: ([SHOW ANSWER](#))

Option D blocks both indicator types at the appropriate enforcement layers. Hard-coded IP callbacks can be matched through a destination IP group referenced by a Cloud Firewall Drop rule, while domain-based callbacks can be denied through a custom URL category and URL Filtering policy. Positioning the specific Firewall denial before generic outbound allows ensures that it is evaluated. Zscaler's Destination IP Group documentation explains how IP addresses, FQDNs, and URL categories are grouped for Firewall policy. The URL Filtering overview documents rules based on URL categories, users, groups, and other criteria. Browser Isolation permits controlled rendering and is not the correct response for confirmed command-and-control infrastructure. TLS inspection alone does not constitute a deny decision. Risk-based page scoring is less deterministic than explicitly blocking known indicators and does not adequately address hard-coded IP callbacks.

NEW QUESTION: 73

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.

Answer: ([SHOW ANSWER](#))

ZPA Access Policies evaluate conditions such as identity, group, posture, location, risk, and client context, then apply an allow or block outcome. Those outcomes can target individual Application Segments or Application Segment Groups. Segment Groups are administrative containers, but policy can still bind access decisions to them. Option C (When a condition is met. an Access Policy can either allow or block access to Application Segments and Application Segment Groups) is correct because Access Policies can allow or block both segments and segment groups when rule conditions match.

Why the other options are incorrect:

- A). When a condition is met, an Access Policy can either allow or block access to Application Segments OR Application Segment Groups: An Application Segment Group is an administrative grouping of app segments used to simplify access policy targeting.
- B). When a condition is met, an Access Policy can allow access to Application Segments Groups and block access to Application Segment: An Application Segment defines private app reachability by FQDN/IP, ports, and related settings.

D). When a condition is met, an Access Policy can allow access to Application Segments and block access to Application Segment Groups: An Application Segment Group is an administrative grouping of app segments used to simplify access policy targeting.

NEW QUESTION: 74

An administrator at a branch observes that a private ERP application is accessible when a user is connected to corporate Wi-Fi but intermittently fails when the user moves to a guest SSID at the same location. Zscaler Client Connector frequently transitions between Forwarding and Bypass states when the network changes.

Which action best reduces the instability?

- A.** Broaden the application segment to include wildcard subdomains so DNS variations do not cause lookup mismatches
- B.** Redesign the Client Connector Forwarding Profile to prioritize stable trusted-network attributes and avoid dependence on volatile SSID-based bypass triggers
- C.** Disable posture checks for the ERP application to prevent frequent re-evaluations from affecting access decisions
- D.** Backhaul all branch traffic to headquarters so users no longer change Service Edges when moving between SSIDs

Answer: ([SHOW ANSWER](#))

Option B targets the evidence: Client Connector changes state whenever network detection changes. Trusted-network classification determines which Forwarding Profile action applies, so criteria that fluctuate during SSID transitions can alternate traffic between forwarding and bypass. The administrator should use stable, independently verifiable criteria such as DNS server, DNS search domain, default gateway, DHCP server, or egress IP, as appropriate for the branch. Zscaler's Trusted Networks overview explains that predefined criteria are selected in Forwarding Profiles, while its Forwarding Profile configuration guide describes how Client Connector verifies trusted networks. Expanding the ERP application segment does not correct state transitions. Disabling posture weakens security without stabilizing forwarding. Backhauling all traffic is disproportionate and retains the underlying unreliable trusted-network definition rather than correcting it.

NEW QUESTION: 75

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: ([SHOW ANSWER](#))

Z-Tunnel 2.0 extends forwarding beyond web proxy traffic by securing all IP unicast traffic through DTLS

/TLS tunnels to the Zero Trust Exchange. This enables Cloud Firewall and other controls to inspect all TCP and UDP ports, and ICMP where supported, rather than only browser HTTP/HTTPS flows. Option C (Zscaler Client Connector will encapsulate the user 's traffic in DTLS/TLS tunnels to the ZTE) is correct because Tunnel 2.0 is the all-ports-and-protocols forwarding model for Client Connector.

Why the other options are incorrect:

A). Zscaler Client Connector will encapsulate the user 's traffic in GRE tunnels to the ZTE:

Zscaler Client Connector is the endpoint agent that steers traffic, authenticates users, reports posture, and supplies ZDX telemetry.

B). Zscaler Client Connector will encapsulate the user 's traffic in IPSec tunnels to the ZTE: IPS inspects traffic inline for exploit signatures and attack patterns, then blocks or resets offending sessions.

D). Zscaler Client Connector will encapsulate the user 's traffic in HTTP Connect tunnels to the ZTE: Zscaler Client Connector is the endpoint agent that steers traffic, authenticates users, reports posture, and supplies ZDX telemetry.

NEW QUESTION: 76

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: (SHOW ANSWER)

Alert Rules can come from Zscaler's ThreatLabZ predefined detections or from customer-defined logic. This lets organizations combine vendor threat intelligence with tenant-specific alerting requirements. Option A (ThreatLabZ pre-defined and customer defined) is correct because the two alert-rule types are ThreatLabZ predefined and customer defined.

Why the other options are incorrect:

B). Snort defined and 3rd party defined: A third-party PageRisk feed would be externally sourced reputation; the Zscaler answer is its own multi-data web-page algorithm.

C). ThreatLabZ pre-defined and 3rd party defined: A third-party PageRisk feed would be externally sourced reputation; the Zscaler answer is its own multi-data web-page algorithm.

D). Customer defined and 3rd party defined: A third-party PageRisk feed would be externally sourced reputation; the Zscaler answer is its own multi-data web-page algorithm.

Valid ZDTA Dumps shared by EduDump.com for Helping Passing ZDTA Exam!

EduDump.com now offer the **newest ZDTA exam dumps**, the EduDump.com ZDTA exam

questions have been updated and answers have been corrected get the **newest** EduDump.com ZDTA dumps with Test Engine here:
<https://www.edudump.com/exams/Zscaler/ZDTA/premium/> (275 Q&As Dumps, **35%OFF**
Special Discount Code: freeexam)

NEW QUESTION: 77

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: (SHOW ANSWER)

Zero Trust connections are designed to be independent of network location as a source of trust. The Zero Trust Exchange brokers access based on identity, device posture, application entitlement, and policy, not on whether the user is inside a static corporate network. Option C (They are independent of any network for control or trust) is correct because control and trust come from policy and context, not from the underlying network.

Why the other options are incorrect:

- A). They require that SSH inspection be enabled: RDP, SSH, and VNC are privileged remote access protocols for desktop, shell, and graphical administration.
- B). They are dependent on a fixed / static network environment: A fixed network dependency is the legacy trust model. Zero Trust removes that dependency by making identity, context, and application policy the trust boundary.
- D). They require IPv6: IPv6 may be supported in parts of a network, but Zero Trust connections do not require IPv6 as a design principle.

NEW QUESTION: 78

When configuring webhook alerts in ZIA, which two webhook authentication types are supported?

- A.** Basic and OAuth
- B.** Token and OAuth
- C.** Basic and Token
- D.** Digest and OAuth

Answer: (SHOW ANSWER)

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

ZIA supports Basic and Token authentication when an administrator adds a webhook, making C correct. With Basic authentication, the configuration supplies a username and password that the receiving endpoint validates. With Token authentication, the administrator provides a bearer token, allowing the destination service to authenticate the webhook request without exposing a username-password pair in each transaction.

OAuth and Digest are not the two authentication selections provided in this ZIA webhook configuration workflow. The distinction matters operationally because the selected method must match the authentication expected by the external notification, automation, or incident-management endpoint. Zscaler's webhook configuration instructions explicitly direct administrators to choose either Basic or Token authentication, then enter the corresponding credentials. Consequently, only option C contains both supported authentication types.

NEW QUESTION: 79

Which of the following can be used as Trusted Network criteria in Zscaler Client Connector?

- A. DNS Server, DHCP Server and Hostname/IP
- B. DHCP Server, DNS Search Domain and Hostname/IP
- C. Hostname/IP, DNS Server and DNS Search Domain
- D. Hostname/IP, DNS Search Domain and DHCP Server

Answer: (SHOW ANSWER)

Trusted Network Detection relies on observable network signals from the endpoint. Hostname/IP resolution, DNS server, and DNS search domain are valid criteria because they indicate whether the device is attached to a known corporate network. Option C (Hostname/IP, DNS Server and DNS Search Domain) is correct because it lists supported trusted-network criteria.

Why the other options are incorrect:

- A). DNS Server, DHCP Server and Hostname/IP: DNS Server criteria identify a trusted network by checking whether the endpoint sees expected internal resolver addresses.
- B). DHCP Server, DNS Search Domain and Hostname/IP: DNS Search Domain is a trusted-network signal because corporate networks commonly push recognizable suffixes to endpoints.
- D). Hostname/IP, DNS Search Domain and DHCP Server: DNS Search Domain is a trusted-network signal because corporate networks commonly push recognizable suffixes to endpoints.

NEW QUESTION: 80

A sanctioned SaaS application is allowed in Cloud App Control but appears to be blocked by URL Filtering.

Which configuration would permit access through a controlled bypass that follows policy precedence?

- A. Move the URL Filtering Allow rule above the Block rule, noting that Cloud App Control-to-URL precedence can still cause an unintended denial
- B. Disable cascading to URL Filtering so Cloud App Control precedence applies and the URL layer does not override the permitted application
- C. Refine Device Posture profile thresholds, acknowledging that posture conditions do not reorder URL policy evaluation
- D. Configure a Trusted Network condition to bypass forwarding, accepting that the block might persist in the URL layer

Answer: B (LEAVE A REPLY)

By default, Cloud App Control takes precedence over URL Filtering when its rule allows a transaction.

Zscaler's URL Filtering configuration documentation explains that enabling Allow Cascading to URL Filtering changes this behavior and causes URL Filtering to evaluate the permitted cloud-application transaction. If that subsequent URL rule blocks the destination, users see the reported denial. Option B restores the intended Cloud App Control decision by disabling cascading for the applicable policy path, preventing the URL layer from overriding the sanctioned application's Allow action. Merely moving a URL Allow rule might affect other sites and does not address why URL Filtering is being invoked. Device posture changes eligibility conditions but not Cloud App Control and URL Filtering precedence. A Trusted Network bypass removes traffic from enforcement and is not a controlled policy correction. The administrator should confirm the matched rules in Web Insights after the change.

NEW QUESTION: 81

An administrator must apply file-type controls to a subset of users while ensuring evasion-resistant detection.

Which configuration most directly maps a file-type policy to a user group and role-based security requirements?

- A. Define a global File Type Control rule that blocks risky formats and rely on identity-based reporting to address group-level differences later
- B. Enable MIME-type validation in a baseline content policy and expect extension mismatches to be handled through application restrictions
- C. Create a File Type Control rule using magic-byte, MIME-type, and file-extension checks; scope it to the target SCIM group and device posture; and place it above broader catch-all rules
- D. Create a URL Filtering rule scoped to the department and reference a custom URL category that lists file extensions for the restricted formats

Answer: ([SHOW ANSWER](#))

Option C combines reliable file identification with precise identity and device scope. The official ZDTA Study Guide describes magic-byte analysis, MIME-type validation, and extension checking. Using all three reduces evasion through renamed extensions or misleading content types. Zscaler's File Type Control documentation supports rules scoped by groups, departments, and locations, so the target SCIM group can receive a stricter policy without imposing it globally. Adding device posture further distinguishes trusted and untrusted endpoints. The specific rule should appear above broader rules so it is evaluated first. A global block ignores role differences. MIME-only inspection leaves gaps when content is mislabeled. URL categories identify destinations, not the true format of transferred files. The combined rule provides the requested role-based and evasion-resistant enforcement.

NEW QUESTION: 82

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

- A. Spyware Callback
- B. Botnet Protection
- C. Blocked Countries

D. Browser Exploits

Answer: ([SHOW ANSWER](#))

Blocked Countries is the Advanced Threat Protection feature used to restrict website access based on geographic location. It gives administrators a geographic control to reduce exposure to destinations associated with embargoed, high-risk, or disallowed regions. Option C (Blocked Countries) is correct because the control is based on country/geography, not malware type.

Why the other options are incorrect:

- A). Spyware Callback: Spyware Callback blocks outbound C2-style communications. It does not describe the browser exploit category in ATP policy.
- B). Botnet Protection: C2/botnet controls detect hosts communicating with known or suspected command- and-control infrastructure.
- D). Browser Exploits: Browser Exploits are attacks against browser vulnerabilities. The question's correct category is the one named by the tested ATP setting, not generic browser exploit handling.

NEW QUESTION: 83

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: ([SHOW ANSWER](#))

For rapid root-cause isolation, ZDX Analyze Score with the Y-Engine is the right diagnostic path. It correlates endpoint, network, Zscaler path, and application metrics so the administrator does not have to manually interpret packet captures or guess whether AWS, Wi-Fi, ISP, or device health is responsible. Option 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) is correct because it gives the fastest useful root-cause analysis from the user 's ZDX score.

Why the other options are incorrect:

- A). Check the Zscaler Trust page for any indications of cloud outages or incidents that would be causing a slowdown: The Zscaler Trust page reports cloud service incidents, but it will not isolate one user's endpoint, Wi-Fi, ISP, or AWS path issue.
- C). Do a Deep Trace on the user 's traffic and check for excessive DNS resolution times and other slowdowns:

DNS resolves names to IP addresses; it is a support service, not an access protocol or scoring engine by itself.

D). Initiate a packet capture from Zscaler Client Connector and escalate the case to have the trace analyzed for root cause: Zscaler Client Connector is the endpoint agent that steers traffic, authenticates users, reports posture, and supplies ZDX telemetry.

NEW QUESTION: 84

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: (SHOW ANSWER)

ZDX Advanced client performance uses live telemetry from real user sessions to measure the experience of internet and private applications. Synthetic probes are useful for availability and path testing, but client performance is gathered by continuously observing active user sessions, endpoint condition, and traffic behavior. Option B (By constantly analyzing live user sessions to both Internet and Private applications and measuring the performance of those sessions) is correct because ZDX Advanced client performance is based on live session analysis.

Why the other options are incorrect:

- A). By generating synthetic transactions to designated Internet and Private applications every 5 minutes and measuring the performance of those sessions: Synthetic transactions are scheduled probes that test applications independently of live user sessions.
- C). By using AI predictive analysis ZDX can extrapolate near-term client performance based upon recent past data observed: AI prediction would forecast likely performance, but the tested ZDX function measures actual client/application sessions.
- D). By constantly analyzing live user sessions to critical SaaS applications and measuring the performance of those sessions: SaaS applications are handled by ZIA controls such as URL Filtering, Cloud App Control, and DLP, not by ZPA App Connectors.

NEW QUESTION: 85

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: (SHOW ANSWER)

Allow Cascading is a layered-policy behavior used when Cloud App Control and URL Filtering both need to evaluate the same transaction. Without cascading, an explicit Cloud App Control allow decision can effectively end processing for that transaction. With cascading enabled, the allowed cloud-app transaction is still passed to URL Filtering so URL category, risk, and isolation decisions can also be enforced. Therefore, Option A (Allow Cascading) is correct because it preserves both application-aware control and destination- category filtering in the same access decision.

Why the other options are incorrect:

B). Allow and Quarantine: Allow and Quarantine would mean access is permitted while content is held or remediated. That is not the feature name for letting URL Filtering run after Cloud App Control allows a transaction.

C). Allow URL Filtering: Allow URL Filtering describes the desired result in plain English. The platform feature name students need to know is Allow Cascading.

D). Allow and Scan: Allow and Scan is a scanning/sandbox-style idea. The Cloud App Control and URL Filtering handoff is specifically called Allow Cascading.

NEW QUESTION: 86

A campaign alert identifies affected users and devices across multiple sites.

Which action should the SOC lead take to strengthen response performance and reduce repetitive manual tasks?

A. Trigger a SOAR playbook through platform APIs to create tickets, block domains in ZIA, and isolate affected endpoints

B. Assign manual triage to each site and postpone enforcement changes until endpoint teams confirm independent findings

C. Disable automated notifications to collaboration tools to reduce noise while analysts evaluate logs for each user separately

D. Increase the alert-severity classification so future campaign alerts appear higher in queues despite limited context enrichment

Answer: (SHOW ANSWER)

Option A converts a correlated campaign finding into consistent, repeatable containment.

Zscaler's Splunk deployment guide documents a sample SOAR playbook that uses NSS data and Zscaler APIs, adds an unclassified malicious domain to the ZIA denylist, and identifies exposed users. Its Microsoft Sentinel deployment guide describes playbooks for URL blocking and endpoint or account containment. The workflow can also create an auditable incident ticket.

Manual site-by-site triage is slower and produces inconsistent handling. Disabling notifications removes coordination without improving evidence. Raising severity changes queue placement but does not contain the threat. Automated actions should still use scoped credentials, required approvals, error handling, and recorded outcomes.

NEW QUESTION: 87

Zscaler utilized a Zero Trust Network Architecture (ZTNA) for segmentation in an environment. Which of the following prevents lateral movement within an organization?

- A. Connect users to applications using Identity, device posture, and access policies
- B. Move all applications into the DMZ
- C. Turn on all host based firewalls
- D. Allow access to all resources on the network via VPN

Answer: ([SHOW ANSWER](#))

Answer A is correct. ZPA uses identity, device posture, application context, and access policy to create a direct connection between an authorized user and a named application. The user is not placed on the private network and is not given routable access to adjacent systems. Zscaler describes this as a "segment of one":

inside-out connectivity and encrypted microtunnels connect the approved user only to the approved application. That design reduces the attack surface and prevents an authenticated or compromised endpoint from discovering and moving to unrelated resources. A DMZ and host firewalls can be useful defense layers, but they do not inherently replace identity-based user-to-application segmentation. A traditional VPN ordinarily extends network-level reach and can increase lateral-movement opportunities. See Zscaler's Private Access data sheet and zero trust architecture overview.

NEW QUESTION: 88

A company requires stricter control of non-web traffic when users are outside the corporate network.

Which adjustment best reduces unintended exposure for off-network users?

- A. Configure Zscaler Client Connector to use Z-Tunnel 2.0 when off-network, and enable the appropriate Cloud Firewall rules
- B. Increase inspection depth for on-network users to compensate for off-network access risks, assuming that stricter internal analysis provides an aggregate deterrent
- C. Configure Zscaler Client Connector to use Z-Tunnel 1.0 when off-network, and enable the appropriate Cloud Firewall rules
- D. Duplicate the off-network block rule and place both copies below the global allow rule to provide redundant coverage and increased monitoring

Answer: ([SHOW ANSWER](#))

Option A forwards the traffic that the organization actually needs to control. Z-Tunnel 2.0 can send all ports and protocols from Zscaler Client Connector to the Zscaler Service Edge, enabling Cloud Firewall to inspect and enforce policy on non-web sessions from roaming users. Zscaler's Z-Tunnel 1.0 and 2.0 documentation confirms that Z-Tunnel 2.0 supports all ports and protocols. Its firewall end-user notification guidance also describes Cloud Firewall handling of non-web traffic over Z-Tunnel 2.0. Tightening on-network inspection does not protect users who are off-network. Z-Tunnel 1.0 primarily handles web proxy traffic and therefore leaves the stated non-web gap. Duplicate rules placed below a global allow will not be reached when the earlier allow rule already matches the session.

NEW QUESTION: 89

How frequently does the Zscaler Client Connector typically check for updates to policy, forwarding, and administration settings?

- A. Every 120 minutes
- B. Every 60 minutes
- C. Every 90 minutes
- D. Every 80 minutes

Answer: ([SHOW ANSWER](#))

Client Connector periodically refreshes policy, forwarding, and administration settings so endpoint behavior aligns with the latest portal configuration. The standard check interval tested here is sixty minutes. Option B (Every 60 minutes) is correct because the client typically checks those settings every 60 minutes.

Why the other options are incorrect:

- A). Every 120 minutes: Every 120 minutes would delay policy, forwarding, and administration setting updates beyond the normal client refresh interval. The tested interval is sixty minutes.
- C). Every 90 minutes: Every 90 minutes is not the standard ZCC refresh interval for policy, forwarding, and administration settings. The tested interval is sixty minutes.
- D). Every 80 minutes: Every 80 minutes is not the normal ZCC setting-refresh cadence. Client Connector typically checks those settings every sixty minutes.

NEW QUESTION: 90

What is the recommended default rule for the cloud-gen firewall configuration when deploying a new ZIA tenant?

- A. Block all traffic
- B. Permit all traffic
- C. Disable the firewall
- D. Allow only web traffic (ports 80/443)

Answer: ([SHOW ANSWER](#))

For a new cloud-gen firewall configuration, a default block posture is the safer baseline.

Administrators should explicitly permit required business traffic and preserve required Zscaler service rules instead of leaving a broad default allow that weakens least-privilege design. Option A (Block all traffic) is correct because block all traffic is the recommended default-deny stance.

Why the other options are incorrect:

- B). Permit all traffic: Permit-all firewall posture lets unexpected services leave the network until later rules stop them.
- C). Disable the firewall: Disabling the firewall removes the enforcement layer instead of creating a safe default rule set.
- D). Allow only web traffic (ports 80/443): Allowing only ports 80/443 would ignore valid non-web business traffic that may need explicit firewall rules.

NEW QUESTION: 91

An operations team wants to determine whether reported slowness in a SaaS application is caused by the application, the network, or the endpoint.

Which ZDX diagnostic should be prioritized to align performance degradation with regions, ISPs, or time windows?

- A. Initiate device-telemetry checks for high CPU utilization and unstable Wi-Fi to flag local constraints before considering path conditions
- B. Run CloudPath probes to capture hop-by-hop latency and packet loss along the end-to-end route to the application
- C. Query Inventory APIs to identify endpoints with older Client Connector builds that may lack recent telemetry capabilities
- D. Review the application's ZDX Score and Page Fetch Time to correlate degradation with geography and time frames

Answer: (SHOW ANSWER)

Option D is the correct starting view for the requested correlation. Zscaler's Performance Dashboard documentation describes both the Regions by ZDX Score map and the Page Fetch Time graph, which tracks how long an application page takes to load over the selected period. The application-details guidance also exposes impacted regions and their probe scores.

Together, these views show whether the degradation is widespread, region-specific, or concentrated in a time window; related ISP incidents can then be examined.

CloudPath is the next drill-down when path evidence is required, while device telemetry tests a particular endpoint hypothesis. Inventory data can reveal version distribution but does not measure the incident. ZDX Score and Page Fetch Time therefore provide the broad correlation needed to choose the correct network, endpoint, or application investigation.

Valid ZDTA Dumps shared by EduDump.com for Helping Passing ZDTA Exam!

EduDump.com now offer the **newest ZDTA exam dumps**, the EduDump.com ZDTA exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ZDTA dumps with Test Engine here:

<https://www.edudump.com/exams/Zscaler/ZDTA/premium/> (275 Q&As Dumps, **35%OFF**

Special Discount Code: freeexam)

NEW QUESTION: 92

A location has a trusted network bypass configured. A Client Connector Forwarding Profile applies category controls and private app access. A new departmental rule is added to permit a niche collaboration suite.

Which action should be taken to mitigate the risk of unintended bypass of inspection for that suite when users are on the trusted network?

- A.** Shift the departmental permit below the global acceptable use controls to discourage inadvertent matches at the edge.
- B.** Refine the trusted network bypass to exclude the collaboration suite ' s domains and ensure the forwarding profile can still apply inspection.
- C.** Reduce the forwarding scope and rely on baseline firewall defaults to constrain traffic during office hours.
- D.** Constrain the forwarding profile by limiting app segments and defer category enforcement until off- network conditions resume.

Answer: ([SHOW ANSWER](#))

Answer B is correct. A Trusted Network bypass can send matching traffic directly instead of forwarding it through the Zscaler enforcement path. If the collaboration suite's domains remain inside that bypass, the departmental permit does not guarantee that category controls or inspection will be applied. The administrator should narrow the bypass so those domains are excluded from direct handling and are forwarded through the profile to ZIA or the appropriate Zscaler service. This preserves the trusted-network behavior for destinations that genuinely require it while restoring inspection for the new suite. Moving the departmental rule does not change traffic that never reaches the policy engine, and firewall defaults cannot substitute for Zscaler inspection. Deferring enforcement off-network also leaves an acknowledged on-network gap. See Zscaler's Forwarding Profile configuration and traffic-forwarding best practices.

NEW QUESTION: 93

A new customer has just purchased Zscaler for Users.

Which of the following Zscaler service entitlements is enabled by default?

- A.** ZPA
- B.** Deception
- C.** ZIA
- D.** ZDX

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

Zscaler Internet Access (ZIA) enrollment is enabled for all users by default, so C is correct.

Zscaler Client Connector service entitlements determine which purchased services are made available to users or device groups. The default ZIA behavior provides Internet and SaaS protection without requiring an administrator to create a selective entitlement rule first. ZPA, ZDX, and Zscaler Deception are separately controlled entitlements and must be enabled according to the organization's licensing and assignment requirements.

They should not be assumed to be active merely because the customer purchased the broader Zscaler for Users offering. Zscaler's service-entitlement documentation explicitly states that ZIA enrollment is always enabled by default. Selective entitlement settings can then target additional services to specific users or device groups.

NEW QUESTION: 94

A team plans to deploy ZPA App Connectors as virtual machines in two data centers and one AWS VPC.

Which information should be communicated upfront to align network placement and access controls with Zero Trust principles?

- A.** The external NAT addresses to advertise for inbound reachability and the BGP communities to tag for internet-facing routes
- B.** The application subnets reachable from connector network interfaces, the requirement for outbound TLS to ZPA Service Edges, and the prohibition of inline TLS interception
- C.** The GRE or IPsec tunnel endpoints that will terminate user traffic at the data-center perimeter for centralized inspection
- D.** The reverse-proxy access control lists that will accept client-initiated TLS from the internet and the static public IP addresses required for allowlists

Answer: ([SHOW ANSWER](#))

Option B states the essential reachability and transport prerequisites. App Connectors must be placed where they can resolve and reach the private applications or subnets assigned to their server groups. Zscaler's App Connector deployment prerequisites specify that, after enrollment, a connector establishes an outbound TLS tunnel over TCP 443 to the ZPA cloud and that TLS interception or inspection must be disabled for this communication. This certificate-pinned, outbound-only design avoids exposing private applications or opening inbound access from the internet. The team must therefore document application-side routing, DNS, firewall egress, and any inspection bypass before deployment in each data center and VPC. GRE and IPsec termination describes other traffic-forwarding designs, not App Connector operation. Reverse-proxy listeners, inbound NAT advertisements, public application addresses, and BGP communities are unnecessary and would conflict with ZPA's reduced attack-surface model.

NEW QUESTION: 95

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

Answer: ([SHOW ANSWER](#))

Advanced Threat Protection defends users from malicious active content, phishing, exploit behavior, C2 callbacks, and risky web destinations. It works as part of ZIA 's inline security stack, often alongside TLS inspection, Cloud Sandbox, DNS security, IPS, and URL categorization.

Option A (Cloud App Control) is correct because malicious active content is the security object ATP is designed to detect and block.

Why the other options are incorrect:

B). URL Filtering: URL Filtering controls web destinations by category, URL, risk, and action such as allow, block, caution, or isolate.

C). Advanced Threat Protection: Advanced Threat Protection blocks malicious active content and related threats. The question is asking for the policy feature named by the configured category, which is not ATP here.

D). Mobile Malware Protection: Mobile Malware Protection focuses on mobile-device malware. The tested ZIA feature is broader web/cloud enforcement rather than mobile-only protection.

NEW QUESTION: 96

Logs indicate traffic to an internal hostname was permitted and not inspected, despite a posture-based access policy that should have blocked the session.

Which statement best explains this outcome?

A. Inspection policy overrode access controls because of protocol heuristics.

B. SAML attribute mapping suppressed posture checks during reauthentication.

C. A Client Forwarding Policy bypass matched first, preventing the access policy from evaluating the session.

D. Connector selection failed closed and defaulted to passthrough to reduce latency.

Answer: C ([LEAVE A REPLY](#))

Answer C is correct. A ZPA Client Forwarding Policy determines whether Client Connector sends application traffic to Private Access or bypasses ZPA. Zscaler documents that these rules use the most-specific application segment and a top-down, first-match principle. If a matching rule bypasses the internal hostname, the connection follows the direct network path and never reaches the ZPA Access Policy that contains the posture condition. Consequently, the access log can show the destination as reachable without the expected ZPA enforcement. An SSL inspection rule cannot override ZPA authorization, and a true fail-closed connector condition would not deliberately pass the session through. The administrator should inspect the matched forwarding rule, application-segment bypass setting, and trusted-network criteria, then remove or narrow the bypass. See Zscaler's Client Forwarding Policy overview and bypass settings guidance.

NEW QUESTION: 97

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: ([SHOW ANSWER](#)**)**

The ZDTA study guide frames common breaches around a four-step lifecycle: discover the attack surface, compromise an entry point, move laterally, and exfiltrate data. Finding the attack surface is the reconnaissance phase in which attackers search for exposed VPNs, firewalls, applications, ports, or public services. Option B (Prevent Compromise) is correct because attack-surface discovery is one of the documented stages.

Why the other options are incorrect:

- A). External Attack Surface: Attack surface is the set of exposed services, addresses, applications, and entry points an attacker can discover.
- C). Data Loss: Data Loss is a Risk360 risk area. The four cyberattack steps in the guide are attack surface, initial compromise, lateral movement, and data exfiltration.
- D). Lateral Propagation: Lateral propagation is a Risk360/risk concept. The attack-lifecycle step named in the guide is lateral movement.

NEW QUESTION: 98

What does Allow Cascading Enabled allow for?

- A. It ensures both Cloud App Control and URL Filtering Rules are applied.
- B. It ensures both Cloud App Control and File Type Control Rules are applied.
- C. It ensures both Cloud App Control and Bandwidth Control Rules are applied.
- D. It ensures both Cloud App Control and DLP Rules are applied.

Answer: A (LEAVE A REPLY)

Allow Cascading is a layered-policy behavior used when Cloud App Control and URL Filtering both need to evaluate the same transaction. Without cascading, an explicit Cloud App Control allow decision can effectively end processing for that transaction. With cascading enabled, the allowed cloud-app transaction is still passed to URL Filtering so URL category, risk, and isolation decisions can also be enforced. Therefore, Option A (It ensures both Cloud App Control and URL Filtering Rules are applied) is correct because it preserves both application-aware control and destination-category filtering in the same access decision.

Why the other options are incorrect:

- B). It ensures both Cloud App Control and File Type Control Rules are applied: File Type Control classifies and restricts uploads or downloads by file type, regardless of filename tricks.
- C). It ensures both Cloud App Control and Bandwidth Control Rules are applied: Cloud Application Control gives application-aware SaaS policy, including activity and tenant-aware restrictions.
- D). It ensures both Cloud App Control and DLP Rules are applied: DLP rules combine detection conditions and policy logic; they are not the content-pattern library itself.

NEW QUESTION: 99

A regional data center experiences intermittent loss of access to an internal ERP application through ZPA during maintenance windows. The site runs two virtual-machine App Connectors mapped to the ERP segment. Maintenance affects one hypervisor at a time, and support tickets show that sessions drop sporadically but recover.

Which change should the ZPA administrator request to improve continuity within the site's constraints?

- A. Reduce application health-check frequency so ZPA waits longer before reassigning sessions during transient failures
- B. Add another App Connector on a separate host to increase the available capacity for session redistribution

C. Increase App Connector CPU reservations to reduce contention spikes during hypervisor maintenance

D. Modify Access Policy priorities to prefer identity attributes that remain stable during maintenance windows

Answer: ([SHOW ANSWER](#))

Option B adds an independent forwarding path outside the hypervisor maintenance domain that is disrupting existing sessions. App Connectors establish outbound connections to ZPA and provide the application-side path for authorized sessions. Zscaler recommends maintaining at least two healthy App Connectors so an available path remains when one connector fails or is unavailable. Its App Connector deployment prerequisites state this minimum explicitly, while the App Connector overview describes their role between application servers and ZPA. Because the observed failure correlates with host maintenance, placing additional capacity on a separate host improves fault-domain diversity and session redistribution. Making health checks less frequent delays failure detection rather than improving availability. CPU reservations do not protect against host maintenance. Identity-policy ordering is unrelated because authentication succeeds; the problem is loss of an application-side connector path.

NEW QUESTION: 100

Operations teams are investigating repeated port-based blocks for outbound traffic and need to correlate the blocked sessions with the applications involved and the applicable Firewall policies. Which steps should the operations team follow?

A. Use Web Insights to examine URL categories and inline web actions for browser traffic

B. Run the URL Test tool to verify static categorization and destination risk scores

C. Review Endpoint DLP Insights to analyze device-level data handling and exfiltration attempts

D. Open Firewall Insights and review rule hits together with application usage and transferred-byte information

Answer: ([SHOW ANSWER](#))

Option D uses the data source built for ZIA Firewall transactions. Firewall Insights records the applied Firewall rule, action, source and destination details, network service, identified network application, and traffic-volume fields. These attributes allow the team to start with blocked ports or services and correlate each event with the responsible rule and detected application. Zscaler's Insights Logs overview states that Firewall logs expose the applied rule, client and server information, network services, and applications. The Firewall Insights column reference documents inbound and outbound byte fields. Web Insights focuses on proxy and web-policy activity rather than general port-based Firewall sessions. The URL Test tool checks categorization but does not reconstruct Firewall enforcement. Endpoint DLP Insights is designed for data-protection events, not application and network-service correlation under Firewall Filtering policy.

NEW QUESTION: 101

How deeply can the Zscaler service scan recursively compressed files for malicious content?

- A. It scans only uncompressed files.
- B. Up to three layers of recursive compression.
- C. Up to two layers of recursive compression.
- D. Up to five layers of recursive compression.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

The Zscaler service can inspect files containing up to five layers of recursive compression, so D is correct.

Recursive archives can conceal malicious executables or documents inside multiple nested containers. ZIA's Malware Protection policy unpacks supported archives layer by layer and scans the extracted content, subject to applicable file-size, file-type, and inspection limitations.

Restricting inspection to uncompressed files, two layers, or three layers would understate the documented capability. Administrators should still combine malware scanning with File Type Control, Cloud Sandbox, Advanced Threat Protection, and controls for encrypted or otherwise unscannable files because recursive-depth support alone does not guarantee that every payload can be inspected. Zscaler's official Malware Protection policy documentation explicitly states that the service scans files with up to five layers of recursive compression.

NEW QUESTION: 102

A Gold-class SaaS application performs poorly even though its bandwidth class has a generous minimum and moderate maximum. Usage dashboards show available capacity during incidents, and other applications are not saturating the link.

What is the most defensible next step to prevent recurring degradation?

- A. Prioritize streaming media above the SaaS application to normalize queue behavior and reduce circuit jitter
- B. Reduce TLS inspection for the SaaS application to remove inspection latency without first validating the traffic path
- C. Raise the Gold-class maximum to a higher ceiling to address presumed internal throttling
- D. Use ZDX path metrics to validate last-mile or ISP congestion at the affected site and plan a circuit upgrade or provider change while retaining the current policies

Answer: ([SHOW ANSWER](#))

The available bandwidth headroom makes policy throttling an unsupported explanation. ZDX should be used to test the remaining network hypothesis before changing security or bandwidth controls. Zscaler's Network Intelligence Dashboard summarizes Last Mile ISP and application performance, while user-detail diagnostics provide CloudPath metrics and links to associated ISP incidents. Repeated latency, packet loss, or jitter on the last-mile or ISP portion during reported failures would support a targeted circuit upgrade, routing correction, or provider change. Raising the class maximum cannot fix congestion outside the organization's controlled queue when capacity is already available. Reducing TLS inspection without evidence creates a security blind spot, and prioritizing streaming media would compete with the business application. Option D

preserves validated policies while collecting evidence for the infrastructure decision that can prevent recurrence.

NEW QUESTION: 103

An investigation at a regional office identifies sensitive files leaving a sanctioned SaaS platform outside business hours. Follow-up analysis shows that several users transferred content through native mobile applications that do not consistently traverse ZIA inline inspection.

Which action should the security lead take next to assess security across the SaaS environment?

- A.** Verify that Browser Isolation is enabled for high-risk sessions and restrict uploads during suspicious activity
- B.** Audit Client Connector posture checks for operating system, disk encryption, and antivirus status to determine whether compliance gates align with DLP enforcement
- C.** Examine DNS telemetry for tunneling to newly registered domains and suppress anomalous outbound queries
- D.** Initiate out-of-band CASB scanning with DLP engines to classify data at rest and review external- sharing configurations across the SaaS tenant

Answer: ([SHOW ANSWER](#))

Option D covers cloud-resident content even when the original transaction did not traverse the inline proxy.

Zscaler's out-of-band CASB uses SaaS-provider API integrations to scan data at rest with DLP engines, identify sensitive content, inspect sharing exposure, and support remediation of risky external shares. Zscaler's Data at Rest Scanning DLP configuration guide places this capability under Out-of-Band CASB. Its CASB overview explains that API-based scanning discovers sensitive SaaS content and that collaboration management can revoke risky sharing. Browser Isolation affects future interactive sessions but does not inventory existing SaaS data. Endpoint posture confirms device compliance rather than classifying tenant content or permissions. DNS analysis addresses command channels and suspicious resolution, not whether sanctioned SaaS files contain regulated data or are shared externally.

NEW QUESTION: 104

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

- A.** Reduce your Internet Attack Surface
- B.** Prevent download of Malicious Files
- C.** Prevent loss to Internet and Cloud Apps
- D.** Securely connect users to Private Applications

Answer: ([SHOW ANSWER](#))

Zscaler Data Protection is primarily adopted to prevent sensitive data from leaving through internet and cloud application channels. The service combines inline DLP, SaaS Security API, endpoint controls, and data discovery to protect data in motion, at rest, and in use. Option C (Prevent loss to Internet and Cloud Apps) is correct because preventing loss to internet and cloud apps is a core data-protection use case.

Why the other options are incorrect:

- A). Reduce your Internet Attack Surface: Attack surface is the set of exposed services, addresses, applications, and entry points an attacker can discover.
- B). Prevent download of Malicious Files: Blocking malicious downloads is threat protection through malware, ATP, sandbox, or file controls rather than DLP for sensitive data loss.
- D). Securely connect users to Private Applications: Secure private-app connectivity is the ZPA use case, not Zscaler Data Protection.

NEW QUESTION: 105

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

- A. Import
- B. LDAP Sync
- C. SCIM
- D. SAML

Answer: ([SHOW ANSWER](#))

SCIM is the open standard for automated identity provisioning and attribute synchronization. It keeps user, group, and department information updated from the IdP into Zscaler without requiring manual edits or waiting for a new SAML login. Option C (SCIM) is correct because SCIM handles automatic updates to identity attributes.

Why the other options are incorrect:

- A). Import: Import is a one-time or manual data-load action. SCIM provides ongoing automated provisioning and synchronization.
- B). LDAP Sync: LDAP queries read structured directory data from Active Directory, such as users, groups, and permissions.
- D). SAML: SAML provides browser-based federation by carrying signed assertions from the identity provider to the service provider.

NEW QUESTION: 106

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: ([SHOW ANSWER](#))

In the Zero Trust Exchange functional services view, Antivirus belongs to the Security Services layer. That layer contains protective inspection capabilities such as antivirus, sandbox, firewall/security inspection, and related threat controls. Option C (Security Services) is correct because Antivirus is a security service, not a platform, access-control, or pure ATP-only category. Why the other options are incorrect:

A). Platform Services: Platform Services provide shared foundations such as policy, identity, and logging.

Antivirus belongs under the security-services protection layer.

B). Access Control Services: Access Control Services handle access, segmentation, and conditional controls.

Antivirus is a threat inspection capability under Security Services.

D). Advanced Threat Prevention Services: Advanced Threat Prevention is a specific threat capability family.

In the functional diagram, Antivirus is grouped more broadly under Security Services.

Valid ZDTA Dumps shared by EduDump.com for Helping Passing ZDTA Exam!

EduDump.com now offer the **newest ZDTA exam dumps**, the EduDump.com ZDTA exam **questions have been updated** and **answers have been corrected** get the **newest**

EduDump.com ZDTA dumps with Test Engine here:

<https://www.edudump.com/exams/Zscaler/ZDTA/premium/> (275 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)

NEW QUESTION: 107

Which field within a URL filtering rule must be defined for Browser Isolation to work?

- A. Groups
- B. User Agent
- C. Departments
- D. Device Trust

Answer: (SHOW ANSWER)

URL Filtering can send traffic to Browser Isolation only when the policy can determine that the user's browser is supported for isolation handling. The User Agent field provides that browser and client context, so it must be defined for Browser Isolation behavior to work correctly in the URL Filtering rule. Option B (User Agent) is correct because User Agent is the required field for applying the isolation action.

Why the other options are incorrect:

- A). Groups: Groups target which users the URL rule applies to. Browser Isolation still needs User Agent so Zscaler can determine browser support/handling.
- C). Departments: Departments are user attributes for rule targeting. They do not tell Zscaler whether the browser session can be isolated.
- D). Device Trust: Device Trust is a posture/context signal. Browser Isolation depends on User Agent information for browser-specific handling.

NEW QUESTION: 108

When correlating indicators of privilege escalation with administrator behavior, which log type provides the most direct visibility into role changes and entitlement modifications for administrative accounts?

- A. Firewall Insights reports centered on rule hits and bandwidth consumption at egress points
- B. ZIdentity Administrator Audit Log filtered for entitlement updates and role assignments
- C. Web Insights transaction logs focusing on URL categories and inline policy actions
- D. Endpoint DLP telemetry summarizing sensitive-data handling and removable-media events

Answer: ([SHOW ANSWER](#))

Answer B is correct. Privilege escalation investigation requires evidence of administrative control-plane actions, especially who changed a role or entitlement, what was changed, and when it occurred. The ZIdentity Administrator Audit Log is the relevant source because Authentication Service centrally manages administrative roles and entitlements across Zscaler services. Filtering that audit trail for role assignments, entitlement updates, and the suspected administrator provides the most direct correlation. Firewall Insights and Web Insights describe data-plane traffic and policy outcomes, while Endpoint DLP telemetry concerns sensitive-data activity; none is the authoritative record of an administrative role change. If the investigation or retention window extends beyond the portal's availability, stream the audit data to the organization's logging platform. See Zscaler's admin roles and permissions and Authentication Service log-streaming guidance.

NEW QUESTION: 109

A managed device on a known corporate LAN cannot reach a private application through the Zero Trust Exchange because of forwarding behavior.

Which bypass configuration would enable access while respecting how policies are evaluated?

- A. Place a broader App Segment earlier in the rule list, conceding that misalignment could widen exposure and still fail to route the session.
- B. Enable a Trusted Network bypass in the Client Forwarding Policy, recognizing that direct access on the corporate LAN limits dependency on ZPA routing.
- C. Apply an Inspection Policy to the application traffic, acknowledging that added parsing may not resolve the routing path.
- D. Introduce an Access Policy allow rule based on group membership, accepting that forwarding mismatches may still block sessions.

Answer: ([SHOW ANSWER](#))

Answer B is correct. When the corporate LAN already provides a valid direct route to the private application, a Trusted Network bypass can tell Client Connector not to forward that application through ZPA on that network. Zscaler supports bypassing ZPA for an application when the user is on a trusted network, and Client Forwarding Policy rules are evaluated using application specificity and top-down, first-match logic. The trusted-network definition and bypass scope must therefore be narrow and stable so that the same traffic is still forwarded and protected when the device leaves the corporate LAN. A broader App Segment changes application matching but does not repair the forwarding path. Inspection Policy affects content handling, and an Access

Policy allow cannot help if traffic never reaches the correct ZPA path. See Zscaler's Client Forwarding Policy overview and client forwarding configuration.

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: (SHOW ANSWER)

After the user receives a valid SAML response from the IdP, ZIA validates the response and issues an authentication token. That token lets Client Connector continue enrollment and policy-controlled access without locally trusting the assertion by itself. Option D (Zscaler Internet Access validates the SAML response and returns an authentication token) is correct because ZIA performs validation and returns the token.

Why the other options are incorrect:

- A). The Zscaler Client Connector Portal authenticates the user directly: Zscaler Client Connector is the endpoint agent that steers traffic, authenticates users, reports posture, and supplies ZDX telemetry.
- B). There is no need for further actions as the SAML is valid, access is granted immediately: SAML provides browser-based federation by carrying signed assertions from the identity provider to the service provider.
- C). The SAML response is sent back to the user's device for local validation: SAML provides browser-based federation by carrying signed assertions from the identity provider to the service provider.

NEW QUESTION: 111

An organization must comply with privacy requirements that restrict decrypting healthcare and financial websites.

Which configuration most precisely implements SSL/TLS bypass for these requirements while preserving inspection elsewhere?

- A. Update DLP policy to redact regulated data after decryption during inline inspection
- B. Redistribute the enterprise root CA to endpoints to strengthen trust and maintain decryption across all categories
- C. Create an SSL/TLS Inspection rule that designates the regulated URL categories as Do Not Inspect and exempts those destinations from decryption
- D. Use out-of-band CASB to quarantine sensitive content discovered at rest in SaaS platforms

Answer: (SHOW ANSWER)

Option C implements the privacy exception in the policy that controls decryption. Zscaler's SSL/TLS Inspection configuration guidance allows rules to use URL Categories as criteria and

apply the appropriate inspection action. Zscaler's rollout best practices specifically note that organizations may bypass the Finance and Health categories because of privacy concerns. A narrowly scoped Do Not Inspect rule for those categories should precede the broader inspection rule, allowing other eligible traffic to remain decrypted and inspected. DLP operates after content becomes visible and therefore cannot satisfy a prohibition on decryption. Root-CA distribution enables trusted interception but does not create a privacy exemption. Out-of- band CASB examines stored SaaS data and does not control the inline TLS session. The exception should also be documented, approved, and periodically reviewed.

NEW QUESTION: 112

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: ([SHOW ANSWER](#))

Zscaler alerting is not limited to email. Alert Rules and detection/response notifications can be sent through webhooks or integrated with collaboration, ITSM, UCaaS, and other third-party tools depending on configuration. Option D (In addition to email, notifications, based on Alert Rules, can be shared with leading ITSM or UCAAS tools over Webhooks) is correct because email and webhook-based integrations support external notification workflows.

Why the other options are incorrect:

- A). Email is the only method for notifications as that is universally applicable and no other way of sending them makes sense: Email and webhooks forward alerts to people or third-party systems for response workflows.
- 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: Email and webhooks forward alerts to people or third-party systems for response workflows.
- 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: NSS is for log streaming to analytics/SIEM destinations. Alert-rule notifications use email and webhook integrations, including ITSM or UCaaS tools.

NEW QUESTION: 113

A new Zscaler Client Connector version causes intermittent tunnel drops for macOS devices in one region during a controlled rollout.

Which action enables broader deployment with minimal disruption while addressing the instability?

- A.** Delay updates in every region until vendor remediation is available, accepting prolonged exposure to vulnerabilities fixed in the new version
- B.** Revert the affected segment to the previous version and continue pilots in unaffected cohorts, monitoring the Zscaler Client Connector dashboard and logs for recurrence
- C.** Reassign every group to an earlier stable version regardless of local stability, sacrificing rollout progress and increasing coordination overhead
- D.** Push diagnostic packet-capture collection to the entire user base, accepting a performance impact for unaffected cohorts

Answer: ([SHOW ANSWER](#))

Option B contains the impact while preserving useful rollout progress. Reverting only the affected macOS regional cohort restores its prior stable state, and continuing controlled pilots elsewhere avoids treating an isolated failure as a universal defect. Dashboard and log monitoring provides evidence about recurrence, affected versions, platforms, and locations before the next expansion decision. Zscaler's Client Connector deployment best practices recommend testing a new version with a defined user group before broad deployment. Its application-update configuration guidance supports managed version rollout. Pausing or reverting every region unnecessarily delays security fixes for stable cohorts. Collecting packet captures from all users is disproportionate and may introduce new performance or privacy concerns; diagnostics should remain targeted to affected endpoints while normal telemetry tracks the wider pilot.

NEW QUESTION: 114

Which of the following features protects traffic to internal applications from attacks such as cross-site scripting (XSS), cookie poisoning, and SQL injection?

- A.** Zscaler Digital Experience
- B.** ZIdentity
- C.** Zscaler Private AppProtection
- D.** Zscaler Cloud Firewall

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

Zscaler Private AppProtection is designed to protect private applications against application-layer attacks, making C correct. It applies inline security inspection to traffic accessing internal web applications and can identify or prevent techniques such as cross-site scripting, SQL injection, and cookie manipulation. This provides protection comparable to web application security controls without exposing the private application directly to the internet. Zscaler Digital Experience monitors performance and user experience but is not the enforcement service for these attacks. ZIdentity provides authentication, identity, and entitlement capabilities.

Zscaler Cloud Firewall enforces network and application traffic policy, but it is not the private-application protection feature described here. The official ZDTA study guide associates Private AppProtection with controls for XSS, SQL injection, and related threats to private applications.

NEW QUESTION: 115

A finance user downloads a password-protected spreadsheet from a sanctioned SaaS platform. Cloud Sandbox indicates that detonation is delayed because the file is encrypted.

Which action should the administrator take next?

- A.** Configure a File Type Control policy to block unscannable files
- B.** Reduce DLP thresholds for the finance department so benign matches are treated as policy violations
- C.** Block tenant-wide access to third-party integrations and suspend the finance user's uploads until further notice
- D.** Move inspection exclusively to API-based scanning and disable inline controls to avoid workflow interruptions

Answer: ([SHOW ANSWER](#))

Option A addresses the precise risk: an encrypted, password-protected file cannot be fully inspected or detonated inline, so it must not be treated as known safe. ZIA can apply a File Type Control action to unscannable files, allowing the organization to block the download according to its risk policy rather than permitting content that malware engines cannot examine. Zscaler's malware-protection security-exception guidance identifies allow or block handling for files that cannot be scanned, and its policy-reason reference includes unscannable-file outcomes. Lowering DLP thresholds targets data-loss detection and would create unrelated false positives. Tenant-wide restrictions are disproportionate to a single encrypted download. API scanning can complement inline inspection for sanctioned SaaS data, but disabling inline control would remove protection at the moment of access and would not make the encrypted file inspectable.

NEW QUESTION: 116

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: ([SHOW ANSWER](#))

Standard SAML browser SSO commonly delivers the assertion to the Service Provider using an HTTP Form POST. The IdP authenticates the user, returns a signed assertion, and the browser posts it to the SP's assertion- consumer endpoint to complete authentication. Option D (Form POST via the browser) is correct because Form POST is the SAML assertion delivery method in this flow.

Why the other options are incorrect:

- A). HTTP Redirect on the browser: HTTP Redirect can start SAML flows, but assertions containing the login result are commonly delivered by browser form POST.
- B). API request/response sequence: An API request/response sequence is server-to-server style integration, not the browser SAML assertion delivery in this scenario.
- C). Through the client connector: Client Connector steers traffic and supports authentication, but it does not replace the browser POST mechanism for the SAML assertion.

NEW QUESTION: 117

What is a key feature of OpenID Connect (OIDC)-based authentication for users?

- A.** It supports attribute-based access control.
- B.** It requires annual certificate maintenance.
- C.** It uses JSON-based web tokens.
- D.** It uses XML to format identity information.

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

OpenID Connect is an identity layer built on OAuth 2.0 and commonly represents identity information in JSON Web Tokens (JWTs), making C correct. A signed ID token carries claims about the authenticated user and can be validated by the relying service using the issuer's published keys. This JSON-based design distinguishes OIDC from SAML, which normally represents assertions in XML. OIDC does not inherently require annual certificate maintenance; signing keys and validation metadata are managed through the provider's configuration and key-discovery mechanisms. Attribute-based access control can consume identity claims, but it is not the protocol characteristic being tested. Zscaler's administrator study material identifies JWTs as JSON-based tokens used in OIDC contexts, and its OpenID configuration documentation explains that attributes are obtained from the OIDC JSON.

NEW QUESTION: 118

What must new administrators in ZIdentity be assigned to perform administrative functions for Zscaler products?

- A.** Service Entitlements
- B.** Just-in-Time (JIT) provisioning
- C.** Environments
- D.** Administrative Entitlements

Answer: ([SHOW ANSWER](#))

Comprehensive and Detailed 100 to 150 words of Explanation From Zscaler Digital Transformation Administrator topics:

New administrators must receive Administrative Entitlements, so D is correct. Administrative Entitlements associate Authentication Service users or groups with subscribed Zscaler services and the administrative roles required to manage those services. Merely existing as a ZIdentity user does not grant product administration privileges. Service Entitlements determine which

Zscaler services end users or device groups can consume; they are not the mechanism for assigning administrator authority. Just-in-Time provisioning can create or update identities during authentication but does not grant the necessary product role by itself. Environments organize applicable service instances but likewise do not replace role assignment. Zscaler's entitlement workflow instructs administrators to select a service on the Administrative Entitlements page and assign users or groups the appropriate administrative roles, ensuring controlled and auditable access.

Valid ZDTA Dumps shared by EduDump.com for Helping Passing ZDTA Exam!

EduDump.com now offer the **newest ZDTA exam dumps**, the EduDump.com ZDTA exam **questions have been updated** and **answers have been corrected** get the **newest** EduDump.com ZDTA dumps with Test Engine here:

<https://www.edudump.com/exams/Zscaler/ZDTA/premium/> (275 Q&As Dumps, **35%OFF**

Special Discount Code: freecram)