Boost up Your Certification Score

Zscaler
ZDTA
Zscaler Digital Transformation Administrator

For More Information – Visit link below:

https://www.examsboost.com/

Product Version

✓ Up to Date products, reliable and verified.
✓ Questions and Answers in PDF Format.

Visit us at: https://www.examsboost.com/test/zdta

Latest Version: 7.2

Question: 1

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: A

Explanation:
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 networks 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.

Question: 2

Which attack type is characterized by a commonly used website or service that has malicious content like malicious JavaScript running on it?

A. Watering Hole Attack
B. Pre-existing Compromise
C. Phishing Attack

D. Exploit Kits

Answer: A

Explanation:
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 A (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:
B . Pre-existing Compromise: Pre-existing compromise means the target is already affected before the current event. A watering-hole attack is different: the attacker poisons a site the victims already visit.
C . Phishing Attack: Phishing starts with social engineering: fake messages, links, or login pages. The question describes a legitimate common website being seeded with malicious JavaScript.
D . 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.

Question: 3

What is the name of the feature that allows the platform to apply URL filtering even when a Cloud App control policy explicitly permits a transaction?

A. Allow Cascading
B. Allow and Quarantine
C. Allow URL Filtering
D. Allow and Scan

Answer: A

Explanation:
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:

Visit us at: https://www.examsboost.com/test/zdta

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.

Question: 4

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: B

Explanation:
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.

Question: 5

Which list of protocols is supported by Zscaler for Privileged Remote Access?

A. RDP, VNC and SSH

B. RDP, SSH and DHCP
C. SSH, DNS and DHCP
D. RDP, DNS and VNC

Answer: A

Explanation:
Zscaler Privileged Remote Access is designed for controlled administrative access to systems without exposing those systems to VPN-style network access. The supported access protocols are the normal privileged-session protocols used by administrators: RDP for Windows desktop administration, SSH for command-line access, and VNC for graphical remote control. That makes Option A (RDP, VNC and SSH) correct. The question is not about general network services; it is about the protocols Zscaler supports for privileged remote sessions through ZPA.
Why the other options are incorrect:
B . RDP, SSH and DHCP: DHCP leases IP addresses to devices. It is useful network plumbing, not a privileged remote access protocol like RDP, SSH, or VNC.
C . SSH, DNS and DHCP: DHCP leases IP addresses to devices. It is useful network plumbing, not a privileged remote access protocol like RDP, SSH, or VNC.
D . RDP, DNS and VNC: DNS resolves names to addresses. Privileged Remote Access needs interactive administration protocols, so DNS is not part of the supported PRA protocol list.

Visit us at: https://www.examsboost.com/test/zdta

Thank You for Trying Our Product

For More Information – Visit link below:

https://www.examsboost.com/

15 USD Discount Coupon Code:

G74JA8UF

FEATURES

- ✓ 90 Days Free Updates
- ✓ Money Back Pass Guarantee
- ✓ Instant Download or Email Attachment
- ✓ 24/7 Live Chat Support
- ✓ PDF file could be used at any Platform
- ✓ 50,000 Happy Customer