

Cisco 300-740

Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT)

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

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



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/300-740>

Latest Version: 6.0

Question: 1

Which security policy is most relevant for controlling access to SaaS applications like Office 365, Workday, and Salesforce?

Response:

- A. Unlimited data transfer policies
- B. Implementing access control based on user identity and device security posture
- C. Allowing all outbound traffic without inspection
- D. Blocking all cloud services to ensure network security

Answer: B

Question: 2

When determining security policies for application enforcement, which of the following is a key consideration?

Response:

- A. The popularity of the application among users
- B. The sensitivity of the data being accessed or stored by the application
- C. The color scheme of the application interface
- D. The programming language used to develop the application

Answer: B

Question: 3

Security services edge (SSE) combines which of the following services for enhanced security at the network edge?

Response:

- A. Secure Web Gateway (SWG)
- B. Cloud Access Security Broker (CASB)
- C. Zero Trust Network Access (ZTNA)
- D. Uninterruptible Power Supply (UPS)

Answer: A,B,C

Question: 4

To allow users a seamless and secure login experience across multiple applications, many organizations configure _____ using an identity provider connection.

Response:

- A. VPNs
- B. firewalls
- C. SAML/SSO
- D. antivirus software

Answer: C

Question: 5

For enforcing application policy at the network security edge, which of the following are critical?

Response:

- A. Enforcing uniform policies without considering individual application requirements
- B. Implementing dynamic security policies based on application behavior and user context
- C. Integrating endpoint security for comprehensive network protection
- D. Ignoring encrypted traffic as it is considered secure

Answer: B,C

Question: 6

What are key considerations when implementing an integrated cloud security architecture?

Response:

- A. Ensuring compatibility between different cloud services
- B. Centralizing all data storage on-premises
- C. Implementing consistent security policies across environments
- D. Leveraging zero-trust principles

Answer: A,C,D

Question: 7

OIDC stands for OpenID Connect. What is it used for in the context of identity management?

Response:

- A. To connect to open networks
- B. To encrypt device data
- C. To authenticate users by leveraging an identity provider
- D. To track user activity on websites

Answer: C

Question: 8

Determine cloud platform security policies based on application connectivity requirements might involve:

Response:

- A. Selecting appropriate cloud service models (IaaS, PaaS, SaaS)
- B. Implementing network peering
- C. Configuring firewalls and access lists
- D. Avoiding the use of security groups and ACLs

Answer: A,B,C

Question: 9

In the context of network protocol blocking, which of the following statements is true?

Response:

- A. Blocking protocols like FTP can prevent unauthorized data transfers
- B. Protocol blocking is an outdated practice that reduces network efficiency
- C. Blocking protocols like BitTorrent can limit the spread of malware
- D. All network protocols should be allowed to ensure maximum compatibility

Answer: A,C

Question: 10

_____ policies are crucial for restricting access to network resources based on the security health of a device.

Response:

- A. Password
- B. Encryption

- C. Endpoint posture
- D. Network segmentation

Answer: C

Thank You for Trying Our Product

Special 16 USD Discount Coupon: NSZUBG3X

Email: support@examsempire.com

**Check our Customer Testimonials and ratings
available on every product page.**

Visit our website.

<https://examsempire.com/>