300-740 Exam Demo - 300-740 Latest Test Question

What's more, part of that SureTorrent 300-740 dumps now are free: https://drive.google.com/open?id=1FvFwE3t2dOHSjLz_4J6kMb7ZSlfkZBn5

You will feel convenient if you buy our product not only because our 300-740 exam prep is of high pass rate but also our service is also perfect. What's more, our update can provide the latest and most useful 300-740 exam guide to you, in order to help you learn more and master more. We provide great customer service before and after the sale and different versions for you to choose, you can download our free demo to check the quality of our 300-740 Guide Torrent before you make your purchase. You will never be disappointed for buying our 300-740 exam questions.

Cisco 300-740 Exam Syllabus Topics:

Topic	Details
Topic 1	• SAFE Key Structure: This section of the exam measures skills of Network Security Designers and focuses on the SAFE framework's key structural elements. It includes understanding 'Places in the Network'—the different network zones—and defining 'Secure Domains' to organize security policy implementation effectively.

Topic 2	• SAFE Architectural Framework: This section of the exam measures skills of Security Architects and explains the Cisco SAFE framework, a structured model for building secure networks. It emphasizes the importance of aligning business goals with architectural decisions to enhance protection across the enterprise.
Topic 3	• Application and Data Security This section of the exam measures skills of Cloud Security Analysts and explores how to defend applications and data from cyber threats. It introduces the MITRE ATT&CK framework, explains cloud attack patterns, and discusses mitigation strategies. Additionally, it covers web application firewall functions, lateral movement prevention, microsegmentation, and creating policies for secure application connectivity in multicloud environments.
Topic 4	• Industry Security Frameworks: This section of the exam measures the skills of Cybersecurity Governance Professionals and introduces major industry frameworks such as NIST, CISA, and DISA. These frameworks guide best practices and compliance in designing secure systems and managing cloud environments responsibly.
Topic 5	• Integrated Architecture Use Cases: This section of the exam measures the skills of Cloud Solution Architects and covers key capabilities within an integrated cloud security architecture. It focuses on ensuring common identity across platforms, setting multicloud policies, integrating secure access service edge (SASE), and implementing zero-trust network access models for more resilient cloud environments.
Topic 6	• User and Device Security: This section of the exam measures skills of Identity and Access Management Engineers and deals with authentication and access control for users and devices. It covers how to use identity certificates, enforce multifactor authentication, define endpoint posture policies, and configure single sign-on (SSO) and OIDC protocols. The section also includes the use of SAML to establish trust between devices and applications.
Topic 7	• Visibility and Assurance: This section of the exam measures skills of Security Operations Center (SOC) Analysts and focuses on monitoring, diagnostics, and compliance. It explains the Cisco XDR solution, discusses visibility automation, and describes tools for traffic analysis and log management. The section also involves diagnosing application access issues, validating telemetry for behavior analysis, and verifying user access with tools like firewall logs, Duo, and Cisco Secure Workload.
Topic 8	• Cloud Security Architecture: This section of the exam measures the skills of Cloud Security Architects and covers the fundamental components of the Cisco Security Reference Architecture. It introduces the role of threat intelligence in identifying and mitigating risks, the use of security operations tools for monitoring and response, and the mechanisms of user and device protection. It also includes strategies for securing cloud and on-premise networks, as well as safeguarding applications, workloads, and data across environments.

>> 300-740 Exam Demo <<

Quiz 2026 Trustable Cisco 300-740: Designing and Implementing Secure Cloud Access for Users and Endpoints Exam Demo

In recent years, the market has been plagued by the proliferation of learning products on qualifying examinations, so it is extremely difficult to find and select our 300-740 test questions in many similar products. However, we believe that with the excellent quality and good reputation of our study materials, we will be able to let users select us in many products. Our study materials allow users to use the 300-740 Certification guide for free to help users better understand our products better. Even if you find that part of it is not for you, you can still choose other types of learning materials in our study materials. We can meet all your requirements and solve all your problems by our 300-740 certification guide.

Cisco Designing and Implementing Secure Cloud Access for Users and Endpoints Sample Questions (Q176-Q181):

NEW QUESTION # 176
Which attack mitigation must be in place to prevent an attacker from authenticating to a service using a brute force attack?

- A. Use of a 100 ms delay between each authentication
- B. Use of a password manager
- C. Use of multifactor authentication for all accounts
- D. Forced password change every 6 months

Answer: C

Explanation:
Multifactor Authentication (MFA) is one of the most effective mitigations against brute-force attacks. Even if an attacker guesses or steals a user's password, they would still need a second authentication factor (e.g., push notification, hardware token, biometric verification) to complete login.
SCAZT Section 2: User and Device Security (Pages 40-43) emphasizes the importance of MFA in protecting identities from password spraying, credential stuffing, and brute-force attacks.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT), Section 2, Pages 40-43

NEW QUESTION # 177

When an application is compromised, the first response action is typically to:

- A. Contain the breach to prevent further unauthorized access
- B. Immediately notify the public
- C. Amplify the breach
- D. Increase user privileges

Answer: A

NEW QUESTION # 178

Utilizing response automation can significantly reduce the time to _____ to incidents, thereby minimizing potential damage.

- A. escalate
- B. contribute
- C. respond
- D. neglect

Answer: C

NEW QUESTION # 179

Refer to the exhibit. An engineer must configure Duo SSO for Cisco Webex and add the Webex application to the Duo Access Gateway. Which two actions must be taken in Duo? (Choose two.)

- A. Upload the SAML application JSON file.
- B. Configure the Applications settings for Cisco Webex.
- C. Add a new application to the Duo platform.
- D. Upload the application XML metadata file.
- E. Import the Identity Provider metadata.

Answer: C,E

Explanation:
To integrate Cisco Webex with Duo SSO using the Duo Access Gateway, the engineer must:
E: Add Cisco Webex as a new SAML application to Duo.
C: Configure the Webex application settings, including Entity ID, Assertion Consumer Service URL, and signing requirements.
Uploading XML metadata (Option A) is typically used when importing IdP settings, not for Duo application configuration. JSON (Option B) is not used in SAML-based Duo app configurations.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT), Section 2:
User and Device Security, Pages 42-45

NEW QUESTION # 180

The integration of SASE in cloud security architecture is aimed at addressing:

- A. The merging of networking and security services to support dynamic secure access
- B. Only the encryption needs of data in transit
- C. The separation of networking and security functions
- D. The reduction of cloud service providers

Answer: A

NEW QUESTION # 181

......