2026 300-740: Perfect Designing and Implementing Secure Cloud Access for Users and Endpoints Practice Tests

BTW, DOWNLOAD part of DumpExam 300-740 dumps from Cloud Storage: https://drive.google.com/open?id=1T6N-oCBstFBXU2r31ANEUhAhinzlywvd

Maybe there are so many candidates think the 300-740 exam is difficult to pass that they be beaten by it. But now, you don't worry about that anymore, because we will provide you an excellent exam material. Our 300-740 exam materials are very useful for you and can help you score a high mark in the test. It also boosts the function of timing and the function to simulate the 300-740 Exam so you can improve your speed to answer and get full preparation for the test. Trust us that our 300-740 exam torrent can help you pass the exam and find an ideal job.

Cisco 300-740 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 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	• 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 6	• Network and Cloud Security:This section of the exam measures skills of Network Security Engineers and covers policy design for secure access to cloud and SaaS applications. It outlines techniques like URL filtering, app control, blocking specific protocols, and using firewalls and reverse proxies. The section also addresses security controls for remote users, including VPN-based and application-based access methods, as well as policy enforcement at the network edge.
Topic 7	• Threat Response: This section of the exam measures skills of Incident Response Engineers and focuses on responding to threats through automation and data analysis. It covers how to act based on telemetry and audit reports, manage user or application compromises, and implement response steps such as containment, reporting, remediation, and reinstating services securely.
Topic 8	• 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.

Real 300-740 Testing Environment - 300-740 Test Collection

The Cisco 300-740 practice exam will be a great help because you are left with little time to prepare for the Cisco 300-740 certification exam which you cannot waste to make time for the Cisco 300-740 Exam Questions. Get the Cisco 300-740 certification by preparing through Cisco 300-740 exam questions that will help you pass the Cisco 300-740 exam.

Cisco Designing and Implementing Secure Cloud Access for Users and Endpoints Sample Questions (Q91-Q96):

NEW QUESTION # 91
Refer to the exhibit. An engineer must provide RDP access to the AWS virtual machines and HTTPS access to the Google Cloud Platform virtual machines. All other connectivity must be blocked. The indicated rules were applied to the firewall; however, none of the virtual machines in AWS and Google Cloud Platform are accessible. What should be done to meet the requirement?

- A. Configure a NAT overload rule
- B. Move rule 1 to the last position
- C. Move rule 2 to the first position.
- D. Configure a virtual private cloud firewall rule

Answer: B

Explanation:
Rule 1 is a "deny all" rule placed at the top of the access control policy. Because Cisco firewalls process rules sequentially from top to bottom, Rule 1 is blocking all traffic-including RDP (Rule 2) and HTTPS (Rule 3).
To allow specific traffic, the "deny all" catch-all rule should be placed last so that the specific allow rules are evaluated first.
SCAZT Section 3 (Network and Cloud Security, Pages 69-74) discusses rule hierarchy and clearly states that allow rules must precede any general deny policies to ensure intended traffic is matched correctly. This best practice is essential when dealing with multi-cloud access control.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT), Section 3, Pages 69-74

NEW QUESTION # 92
The main benefit of integrating threat intelligence into cloud security is:

- A. Decreasing the need for secure domains
- B. Increasing the complexity of security architectures
- C. Reducing the effectiveness of security operations
- D. Enhancing the ability to identify and respond to emerging threats

Answer: D

NEW QUESTION # 93
Refer to the exhibit. An engineer must provide HTTPS access from the Google Cloud Platform virtual machine to the on-premises mail server. All other connections from the virtual machine to the mail server must be blocked. The indicated rules were applied to the firewall; however, the virtual machine cannot access the mail server. Which two actions should be performed on the firewall to meet the requirement? (Choose two.)

- A. Move up rule 2.
- B. Set IP address 20.1.1.1 as the source in rule 1.
- C. Configure a NAT rule.
- D. Set IP address 192.168.200.10 as the destination in rule 1.
- E. Configure a security group.

Answer: C,D

Explanation:
From the firewall access rules provided, Rule 1 allows traffic from 20.1.1.10 (GCP VM) to 20.1.1.1 using HTTPS. However, this destination is not the actual mail server-the mail server resides at 192.168.200.10 (inside network). Therefore:
A: Rule 1 must be updated to reflect the correct destination: 192.168.200.10. Without this change, traffic is not permitted to the mail server.
D: NAT (Network Address Translation) is needed to translate the external address (e.g., 20.1.1.10) to access internal addresses (like 192.168.200.10). As per SCAZT and Cisco firewall policies, NAT enables proper packet delivery from public to private zones.
Rule 2, which denies all other traffic, is correctly placed after the specific allow rule. Therefore, moving it (Option B) would not help, and Options C and E are unrelated to resolving the immediate firewall access and routing issue.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT), Section 3:
Network and Cloud Security, Pages 72-77

NEW QUESTION # 94
Refer to the exhibit. A security engineer deployed Cisco Secure XDR, and during testing, the log entry shows a security incident. Which action must the engineer take first?

- A. Isolate the endpoint.
- B. Block IP address 10.77.17.45.
- C. Rebuild the endpoint.
- D. Uninstall the malware.

Answer: A

Explanation:
The SCAZT documentation emphasizes that when Cisco Secure XDR identifies a high-risk threat (e.g., risk score 8 out of 10 for malware distribution, as shown in the exhibit), the first priority is to prevent lateral movement and data exfiltration. The recommended first response action is to isolate the affected endpoint from the network.
Cisco Secure Endpoint and XDR allow you to trigger an "isolate" response directly from the dashboard, cutting off all non-management communication from the compromised device. This preserves the environment and enables forensic analysis before removing malware or taking destructive actions like rebuilding the system.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT), Section 6:
Threat Response, Pages 113-118

NEW QUESTION # 95
According to Cisco Security Reference Architecture, which solution provides threat intelligence and malware analytics?

- A. Cisco Talos
- B. Cisco Umbrella
- C. Cisco pxGrid
- D. Cisco XDR

Answer: A

Explanation:
Cisco Talos is Cisco's threat intelligence organization, delivering real-time threat intelligence and malware analytics to help organizations detect and prevent threats before they impact the network. According to the SCAZT guide, Talos provides comprehensive coverage of threat data including signatures, indicators of compromise, and context-driven analytics. This intelligence feeds into Cisco security platforms such as Cisco SecureX and Cisco Secure Endpoint to enhance detection, investigation, and response capabilities. Talos is explicitly referenced in the Threat Response section as the primary source of threat intelligence and malware analytics that supports cloud and endpoint security frameworks.
Reference: Designing and Implementing Secure Cloud Access for Users and Endpoints (SCAZT) Study Guide, Section 6: Threat Response, Pages 112-115.

NEW QUESTION # 96
.....

The second format is a web-based format that can be accessed from browsers like Firefox, Microsoft Edge, Chrome, and Safari. It means you don't need to download or install any software or plugins to take the Designing and Implementing Secure Cloud Access for Users and Endpoints practice test. The web-based format of the Cisco 300-740 Certification Exams practice test supports all operating systems. The third and last format is desktop software format which can be accessed after installing the software on your Designing and Implementing Secure Cloud Access for Users and Endpoints (300-740) Windows Pc or Laptop. These formats are built especially for the students so they don't stop preparing for the Designing and Implementing Secure Cloud Access for Users and Endpoints (300-740) certification.

www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, zenwriting.net, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

What's more, part of that DumpExam 300-740 dumps now are free: https://drive.google.com/open?id=1T6N-oCBstFBXU2r31ANEUhAhinzlywvd