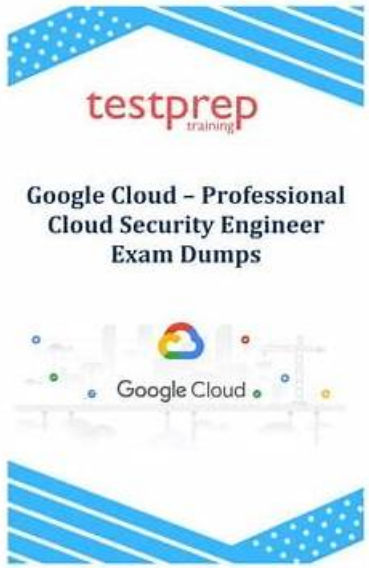
Examcollection Professional-Cloud-Security-Engineer Dumps Torrent & Trustworthy Professional-Cloud-Security-Engineer Source



P.S. Free 2026 Google Professional-Cloud-Security-Engineer dumps are available on Google Drive shared by Real4exams: https://drive.google.com/open?id=1TroGT_uWeP2_5lVYmIQEfrSwcj_hlxvm

Pass the Google Cloud Certified - Professional Cloud Security Engineer Exam Professional-Cloud-Security-Engineer certification exam which is a challenging task. To make Professional-Cloud-Security-Engineer exam success journey simple, quick, and smart, you have to prepare well and show a firm commitment to passing this exam. The real, updated, and error-free Google Cloud Certified - Professional Cloud Security Engineer Exam Professional-Cloud-Security-Engineer Exam Dumps are available over the Real4exams.

Real4exams designed this prep material to help you pass the exam on the first try. It may sound complicated, but once you go through regular study and intensive practice, passing the final exam would be a piece of cake. The cost of Google Cloud Certified - Professional Cloud Security Engineer Exam (Professional-Cloud-Security-Engineer) certification itself is expensive, ranging from $100 to $1000, so you can't risk wasting that amount. Real4exams ensures that this does not happen by providing you with reliable and updated preparation material.

>> Examcollection Professional-Cloud-Security-Engineer Dumps Torrent <<

Pass Guaranteed Google First-grade Professional-Cloud-Security-Engineer - Examcollection Google Cloud Certified - Professional Cloud Security

Engineer Exam Dumps Torrent

We provide the update freely of Professional-Cloud-Security-Engineer Exam Questions within one year and 50% discount benefits if buyers want to extend service warranty after one year. The old client enjoys some certain discount when buying other exam materials. We update the Professional-Cloud-Security-Engineer guide torrent frequently and provide you the latest study materials which reflect the latest trend in the theory and the practice. So you can master the Google Cloud Certified - Professional Cloud Security Engineer Exam test guide well and pass the exam successfully. While you enjoy the benefits we bring you can pass the exam.

To be eligible for the exam, candidates should have at least three years of experience in IT security, including one year of experience in designing and managing solutions on the Google Cloud Platform. They should also have a good understanding of security principles and concepts, such as identity and access management, encryption, and incident response.

The Google Professional-Cloud-Security-Engineer Exam covers a wide range of topics, including security management, data protection, network security, and compliance. Candidates are expected to have a deep understanding of the security controls and mechanisms available on the Google Cloud Platform. They should also be able to identify and mitigate potential security threats and vulnerabilities.

What is the Passing Score, Duration & Questions for the GoogleProfessional Cloud Security Engineer Exam

- Length of Examination: 120 minutes
- Passing score: N/A
- Format: Multiple choices, multiple answers
- Number of Questions: 50-60
- Language: English

Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q47-Q52):

NEW QUESTION # 47
A large e-retailer is moving to Google Cloud Platform with its ecommerce website. The company wants to ensure payment information is encrypted between the customer's browser and GCP when the customers checkout online.
What should they do?

- A. Configure an SSL Certificate on an L7 Load Balancer and require encryption.
- B. Configure an SSL Certificate on a Network TCP Load Balancer and require encryption.
- C. Configure the firewall to allow inbound traffic on port 443, and block all other inbound traffic.
- D. Configure the firewall to allow outbound traffic on port 443, and block all other outbound traffic.

Answer: A

Explanation:
https://cloud.google.com/load-balancing/docs/load-balancing-overview#external_versus_internal_load_balancing

NEW QUESTION # 48
Your company is developing a new application for your organization. The application consists of two Cloud Run services, service A and service B. Service A provides a web-based user front-end. Service B provides back-end services that are called by service A. You need to set up identity and access management for the application. Your solution should follow the principle of least privilege.
What should you do?

- A. Create two separate service accounts. Grant one service account the permissions to execute service A, and grant the other service account the permissions to execute service B. Require authentication for service B. Permit only the service account for service A to call the back-end.
- B. Use the Compute Engine default service account to run service A and service B. Require authentication for service B. Permit only the default service account to call the backend.
- C. Create a new service account with the permissions to run service A and service B. Require authentication for service B. Permit only the new service account to call the backend.
- D. Create three separate service accounts. Grant one service account the permissions to execute service A.Grant the second

service account the permissions to run service B. Grant the third service account the permissions to communicate between both services A and B. Require authentication for service B. Call the back-end by authenticating with a service account key for the third service account.

Answer: A

Explanation:
The problem describes an application with two Cloud Run services (Service A - frontend, Service B - backend) and requires setting up IAM with the principle of least privilege. Service A calls Service B.
Principle of Least Privilege: This principle dictates that each entity (in this case, a Cloud Run service) should only have the minimum permissions necessary to perform its function.
Separate Service Accounts for Separate Services: To adhere to the principle of least privilege, it's best practice to assign a unique service account to each distinct service or component. This ensures that a compromise of one service account does not grant excessive permissions across other services. Service A needs permissions to run itself and to invoke Service B. Service B only needs permissions to run itself.Extract Reference:
"Assign a service account to a Cloud Run service. The service account acts as the identity for your service and determines what permissions your revisions have when executing requests. It is a best practice to grant each service account only the permissions that are required to run the specific service (principle of least privilege)." (Google Cloud documentation: https://cloud.google.com/run/docs/configuring/service-accounts) Authentication for Cloud Run Services: When one Cloud Run service (caller) needs to invoke another Cloud Run service (callee), the caller must be authorized to do so. This is typically achieved by assigning the roles
/run.invoker role on the callee service to the caller's service account.Extract Reference: "To allow a service to invoke another service, grant the roles/run.invoker role on the called service to the caller's service account." (Google Cloud documentation: https://cloud.google.com/run/docs/securing/service-to-service) Let's evaluate the options:
A). Create a new service account with the permissions to run service A and service B. Require authentication for service B. Permit only the new service account to call the backend. This violates the principle of least privilege by giving a single service account permissions for both services. If that service account were compromised, both services would be affected.
B). Create two separate service accounts. Grant one service account the permissions to execute service A, and grant the other service account the permissions to execute service B. Require authentication for service B.
Permit only the service account for service A to call the back-end. This aligns perfectly with least privilege.
Service A gets its own identity, Service B gets its own identity. Service A's service account is then granted run.invoker permissions on Service B, allowing it to call the backend while Service B requires authentication.
This is the recommended approach.
C). Use the Compute Engine default service account to run service A and service B. Require authentication for service B. Permit only the default service account to call the backend. The Compute Engine default service account often has broad permissions (e.g., editor role in its project). Using it violates the principle of least privilege and is generally discouraged for production applications due to the potential for excessive permissions.
D). Create three separate service accounts. Grant one service account the permissions to execute service A.
Grant the second service account the permissions to run service B. Grant the third service account the permissions to communicate between both services A and B. Require authentication for service B. Call the back-end by authenticating with a service account key for the third service account. This introduces unnecessary complexity with a third service account just for communication. More critically, using a service account key for authentication is generally discouraged in Cloud Run environments where ADC (Application Default Credentials) can be used, as managing keys securely becomes an operational overhead and security risk. Cloud Run services automatically use their attached service accounts for authentication when making calls to other Google Cloud services, including other Cloud Run services.
Therefore, option B is the best solution, adhering to the principle of least privilege and Google Cloud best practices for Cloud Run service-to-service authentication.

NEW QUESTION # 49
You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow thee application frontend to access the data in the application's mysql instance on port 3306. What should you do?

- A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag "data-tag" that is applied to the mysql Compute Engine VM on port 3306.
- B. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged fe-tag.
- C. Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique

service account of the mysql Compute Engine VM on port 3306.
- D. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

Answer: A

Explanation:
To restrict access to the MySQL instance to only the frontend application while other VMs are present in the subnets, creating an ingress firewall rule is the most appropriate approach. This rule will specifically allow traffic from subnet A (where the frontend application resides) to the MySQL instance in subnet B on port
3306, using network tags to target the specific MySQL VM.
Steps:
* Create Network Tags: Apply a network tag (e.g., "data-tag") to the MySQL VM in subnet B.
* Create Ingress Firewall Rule: Configure an ingress firewall rule with the following settings:
* Source IP Range: Subnet A's IP range.
* Target Tag: "data-tag".
* Allowed Protocol/Ports: TCP:3306 (for MySQL).
This setup ensures that only instances in subnet A can communicate with the MySQL instance on port 3306.
References:
* Google Cloud: Configuring firewall rules

NEW QUESTION # 50
You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment.
How should you prevent and fix this vulnerability?

- A. Use Web Security Scanner to validate the usage of an outdated library in the code, and then use a secured version of the included library.
- B. Use Cloud IAP based on IP address or end-user device attributes to prevent and fix the vulnerability.
- C. Set up an HTTPS load balancer, and then use Cloud Armor for the production environment to prevent the potential XSS attack.
- D. Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping.

Answer: D

Explanation:
Web Security Scanner cross-site scripting (XSS) injection testing *simulates* an injection attack by inserting a benign test string into user-editable fields and then performing various user actions.
https://cloud.google.com/security-command-center/docs/how-to-remediate-web-security-scanner- findings#xss

NEW QUESTION # 51
Your Security team believes that a former employee of your company gained unauthorized access to Google Cloud resources some time in the past 2 months by using a service account key. You need to confirm the unauthorized access and determine the user activity. What should you do?

- A. Use the Cloud Monitoring console to filter audit logs by user.
- B. Use the Cloud Data Loss Prevention API to query logs in Cloud Storage.
- C. Use Security Health Analytics to determine user activity.
- D. Use the Logs Explorer to search for user activity.

Answer: D

Explanation:
* Objective: Ensure that a Cloud Storage bucket in Project A can only be readable from Project B and prevent data access or copying to Cloud Storage buckets outside the network, even with correct credentials.
* Solution: Use VPC Service Controls to create a security perimeter.

* Steps:
* Step 1: Open the Google Cloud Console.
* Step 2: Navigate to the VPC Service Controls page.
* Step 3: Create a new service perimeter.
* Step 4: Add Project A and Project B to the service perimeter.
* Step 5: Include Cloud Storage service in the perimeter configuration.
* Step 6: Define access levels to ensure that only resources within the perimeter can access the Cloud Storage bucket.
By setting up a VPC Service Controls perimeter, you can enforce security boundaries that restrict data access and movement to within defined projects, providing an extra layer of protection beyond IAM permissions.
References:
* VPC Service Controls Overview
* Configuring VPC Service Controls

NEW QUESTION # 52
.....

The Professional-Cloud-Security-Engineer training vce offered by Real4exams will be the best tool for you to pass your actual test. The Professional-Cloud-Security-Engineer questions & answers are especially suitable for the candidates like you for the coming exam test. The contents of Google study dumps are edited by our experts who have rich experience, and easy for all of you to understand. So, with the skills and knowledge you get from Professional-Cloud-Security-Engineer practice pdf, you can 100% pass and get the certification you want.

Engineer Test Engine

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

BTW, DOWNLOAD part of Real4exams Professional-Cloud-Security-Engineer dumps from Cloud Storage: https://drive.google.com/open?id=1TroGT_uWeP2_5lVYmIQEfrSwcj_hlxvm