Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

Go to Exam

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 299 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 299

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You manage multiple internal-only applications that are hosted within different Google Cloud projects. You are deploying a new application that requires external internet access. To maintain security, you want to clearly separate this new application from internal systems. Your solution must have effective security isolation for the new externally-facing application. What should you do?

A. Deploy the application within the same project as an internal application. Use a Shared VPC model to manage network configurations.

B. Place the application in the same project as an existing internal application, and adjust firewall rules to allow external traffic.

C. Create a VPC Service Controls perimeter, and place the new application’s project within that perimeter.

D. Create a new project for the application, and use VPC Network Peering to access necessary resources in the internal projects.

Show Suggested Answer

by abdelrahman89 at *Oct. 4, 2024, 9:54 p.m.*

Comments

Type your comment...

Submit

YourFriendlyNeighborhoodSpider 4 months, 1 week ago

Selected Answer: D

Answer is D, because that way you have complete isolation as required in the question.
Explanation for C:
C. Use VPC Service Controls (VPC-SC) is useful for protecting data from being exfiltrated, but it does not isolate an externally-facing app from internal systems. It is more suited for controlling access to sensitive APIs and services, not for network-level isolation.

upvoted 2 times

p981pa123 6 months, 1 week ago

Selected Answer: C

You need stronger security and isolation for the externally-facing application and want to prevent unintended data access or leakage.

upvoted 1 times

LaxmanTiwari 7 months ago

Selected Answer: D

Agree with Pime13

upvoted 2 times

Pime13 7 months, 3 weeks ago

Selected Answer: D

Option C suggests creating a VPC Service Controls perimeter and placing the new application's project within that perimeter. While VPC Service Controls can enhance security by defining a security perimeter around Google Cloud resources, it is primarily designed to protect data from being exfiltrated to unauthorized networks or users. It does not inherently provide the level of isolation needed for an externally-facing application.

Creating a new project (Option D) ensures complete separation of resources, IAM policies, and network configurations, which is crucial for maintaining security isolation between internal and external applications. This approach minimizes the risk of accidental exposure of internal resources to the internet.

upvoted 2 times

vamgcp 8 months ago

Selected Answer: D

While VPC Service Controls offer strong isolation, they might be overkill for this scenario involving internal applications with moderate security needs.

upvoted 2 times

f36bdb5 8 months, 2 weeks ago

Selected Answer: C

It does not say anywhere that the external application should access internal resources. VPC peering would then be a massive security risk

upvoted 4 times

> **MoAk** 8 months ago
>
> Indeed. AND the Q clearly states 'effective security isolation'. This is VPC SCs
>
> upvoted 2 times

json4u 9 months, 2 weeks ago

Selected Answer: D

It's D

upvoted 1 times

abdelrahman89 9 months, 3 weeks ago

D - Dedicated Project: Creating a new project for the externally-facing application provides a clear separation from internal systems, reducing the risk of unauthorized access or lateral movement.
VPC Network Peering: Using VPC Network Peering allows the new project to access resources in the internal projects, while maintaining a controlled and secure boundary. This ensures that external traffic cannot directly access internal resources without going through the established peering connection.
Improved Security: This approach offers enhanced security by minimizing the attack surface and limiting the potential impact of a breach.

upvoted 1 times

Platform

- Home
- Examtopics PRO
- All Exams
- Training Courses