Google Discussions

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 256 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 256

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your organization has two VPC Service Controls service perimeters, Perimeter-A and Perimeter-B, in Google Cloud. You want to allow data to be copied from a Cloud Storage bucket in Perimeter-A to another Cloud Storage bucket in Perimeter-B. You must minimize exfiltration risk, only allow required connections, and follow the principle of least privilege. What should you do?

A. Configure a perimeter bridge between Perimeter-A and Perimeter-B, and specify the Cloud Storage buckets as the resources involved.

B. Configure a perimeter bridge between the projects hosting the Cloud Storage buckets in Perimeter-A and Perimeter-B.

C. Configure an egress rule for the Cloud Storage bucket in Perimeter-A and a corresponding ingress rule in Perimeter-B.

D. Configure a bidirectional egress/ingress rule for the Cloud Storage buckets in Perimeter-A and Perimeter-B.

Show Suggested Answer

by yokoyan at *Sept. 6, 2024, 1:25 a.m.*

Comments

Type your comment...

Submit

⊟ YourFriendlyNeighborhoodSpider 4 months, 1 week ago

Selected Answer: C

"minimize exfiltration risk, only allow required connections, and follow the principle of least privilege" - C follow the principle of least privilege
While a perimeter bridge allows communication between two service perimeters, it may grant broader access than necessary and does not adhere to the principle of least privilege, as it could expose resources to more connections than intended.

upvoted 1 times

KLei 7 months, 1 week ago

Selected Answer: C

"minimize exfiltration risk, only allow required connections, and follow the principle of least privilege" - C follow the principle of least privilege

upvoted 2 times

> **KLei** 7 months, 1 week ago
>
> While a perimeter bridge allows communication between two service perimeters, it may grant broader access than necessary and does not adhere to the principle of least privilege, as it could expose resources to more connections than intended.
>
> upvoted 1 times

Pime13 7 months, 3 weeks ago

Selected Answer: A

https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters#example_of_perimeter_bridges

upvoted 1 times

cachopo 7 months, 3 weeks ago

Selected Answer: A

A perimeter bridge allows limited communication between resources in two service perimeters. By explicitly specifying the Cloud Storage buckets involved, you restrict the scope of the bridge to only the required resources.

While egress and ingress rules control data flow, they are typically used for access to services outside the perimeters, not between two perimeters. Additionally, this approach lacks granularity and risks unintended exposure.

upvoted 1 times

> **cachopo** 7 months, 3 weeks ago
>
> Also, this is pretty similar to the example exposed in the documentation:
>
> https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters#example_of_perimeter_bridges
>
> upvoted 1 times

BPzen 8 months ago

Selected Answer: A

To enable data transfer between two VPC Service Controls service perimeters while minimizing exfiltration risk and adhering to the principle of least privilege, you need to use a perimeter bridge. This bridge allows controlled communication between the two perimeters but must be configured to include only the specific resources (in this case, the Cloud Storage buckets).

Here's why the other options are less suitable:
A perimeter bridge between projects is overly broad and does not align with the principle of least privilege. It would allow communication for all resources in the projects, increasing the risk of exfiltration.
C. Configure an egress rule for the Cloud Storage bucket in Perimeter-A and a corresponding ingress rule in Perimeter-B.

VPC Service Controls do not directly support simple egress/ingress rules between perimeters. Perimeter bridges are the designed mechanism for controlled inter-perimeter communication.

upvoted 1 times

nah99 8 months ago

Selected Answer: C

https://cloud.google.com/vpc-service-controls/docs/ingress-egress-rules

upvoted 2 times

MoAk 8 months, 1 week ago

Selected Answer: A

Looks like this chat has been infiltrated. Clearly the correct answer is A. this exact feature exists for this use case.

upvoted 2 times

> **nah99** 8 months ago
>
> Nope, C is better.
>
> "Ingress and egress rules can replace and simplify use cases that previously required one or more perimeter bridges."

"Minimize exfiltration risk by constraining the exact service, methods, Google Cloud projects, VPC networks, and identities used to execute the data exchange."

https://cloud.google.com/vpc-service-controls/docs/ingress-egress-rules

upvoted 2 times

MoAk 8 months ago

This is the way. Thanks :)

"Ingress and egress rules can replace and simplify use cases that previously required one or more perimeter bridges."

Answer C

upvoted 1 times

jmaquino 8 months, 2 weeks ago

Selected Answer: C

C: Data exchange between clients and resources separated by perimeters is secured by using ingress and egress rules. https://cloud.google.com/vpc-service-controls/docs/overview

upvoted 2 times

BondleB 8 months, 4 weeks ago

Selected Answer: C

C

upvoted 2 times

d0fa7d5 10 months, 3 weeks ago

Selected Answer: A

I think B is too broad in scope.

upvoted 4 times

BB_norway 10 months, 3 weeks ago

Selected Answer: C

It should be C, due to the offered granular control and principle of least priviledge

upvoted 4 times

yokoyan 10 months, 3 weeks ago

Selected Answer: B

I think it's B.

upvoted 1 times

EXAMTOPICS

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses