

[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 150 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 150

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

Your organization's Google Cloud VMs are deployed via an instance template that configures them with a public IP address in order to host web services for external users. The VMs reside in a service project that is attached to a host (VPC) project containing one custom Shared VPC for the VMs. You have been asked to reduce the exposure of the VMs to the internet while continuing to service external users. You have already recreated the instance template without a public IP address configuration to launch the managed instance group (MIG). What should you do?

- A. Deploy a Cloud NAT Gateway in the service project for the MIG.
- B. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.
- C. Deploy an external HTTP(S) load balancer in the service project with the MIG as a backend.
- D. Deploy an external HTTP(S) load balancer in the host (VPC) project with the MIG as a backend.

[Show Suggested Answer](#)

by [deleted] at *Sept. 6, 2022, 6:36 a.m.*

Comments

[Submit](#)

🗑️ 👤 **Littleivy** Highly Voted 👍 2 years, 8 months ago

Selected Answer: C

Answer is C

NAT is for egress. To serve customers, need to have LB in the same project

👍 ↩️ 🚩 upvoted 14 times

🗑️ 👤 **GHOST1985** Highly Voted 👍 2 years, 8 months ago

Selected Answer: C

No doubt the answer is C, this is the Two-tier web service model , below the example from google cloud documentation https://cloud.google.com/vpc/docs/shared-vpc#two-tier_web_service

👍 ↩️ 🚩 upvoted 7 times

🗑️ 👤 **LaithTech** Most Recent 🕒 11 months, 2 weeks ago

Selected Answer: D

Based on the network architecture and best practices for managing resources in a Shared VPC environment. Answer is D

👍 ↩️ 🚩 upvoted 1 times

🗑️ 👤 **winston9** 1 year, 6 months ago

Selected Answer: C

using an external HTTP(S) load balancer deployed within the service project, where the VMs reside, offers the most secure, efficient, and organizationally aligned solution for achieving your objective of minimizing internet exposure while maintaining external user access to your web services.

👍 ↩️ 🚩 upvoted 2 times

🗑️ 👤 **gical** 1 year, 7 months ago

Answer is C.

<https://cloud.google.com/load-balancing/docs/https#shared-vpc>

For the Application Load Balancer: "The regional external IP address, the forwarding rule, the target HTTP(S) proxy, and the associated URL map must be defined in the same project. This project can be the host project or a service project." The question is mentioning "VMs reside in a service project" and "have been asked to reduce the exposure of the VMs"

👍 ↩️ 🚩 upvoted 2 times

🗑️ 👤 **TNT87** 2 years, 3 months ago

<https://cloud.google.com/architecture/building-internet-connectivity-for-private-vms#objectives>

👍 ↩️ 🚩 upvoted 1 times

🗑️ 👤 **fad3r** 2 years, 4 months ago

The people who think it is cloud nat really do not have a fundamental grasp on how networking / natting actually work

👍 ↩️ 🚩 upvoted 2 times

🗑️ 👤 **shayke** 2 years, 7 months ago

Selected Answer: C

C is the right ans

👍 ↩️ 🚩 upvoted 2 times

🗑️ 👤 **AzureDP900** 2 years, 8 months ago

B. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.

👍 ↩️ 🚩 upvoted 1 times

🗑️ 👤 **GHOST1985** 2 years, 8 months ago

How Cloud NAT could be able to expose internal IP to the public users !! please refers to the documentation before answering !

<https://cloud.google.com/nat/docs/overview>

👍 ↩️ 🚩 upvoted 3 times

🗑️ 👤 **AzureDP900** 2 years, 8 months ago

Thank you for sharing link, I am changing it to C

👍 ↩️ 🚩 upvoted 1 times

🗑️ 👤 **coco10k** 2 years, 8 months ago

Selected Answer: C

recently support for host project LBs was introduced but usually the LB stays with the backend services in the service project. so answer C

👍 ↩️ 🚩 upvoted 4 times

🗑️ 👤 **asdf12345678** 2 years, 8 months ago

the official doc still does not support frontend / backend of global https LB in different projects. so +1 to C (https://cloud.google.com/load-balancing/docs/features#network_topologies)

(https://cloud.google.com/load-balancing/docs/features#network_topologies)

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **Table2022** 2 years, 9 months ago

Answer is C, The first example creates all of the load balancer components and backends in the service project.
<https://cloud.google.com/load-balancing/docs/https/setting-up-reg-ext-shared-vpc>

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **crisyeb** 2 years, 9 months ago

Selected Answer: C

For me C is the answer.

Cloud NAT is for outbound traffic and LB is to handle external customers' request to web services, so it is a LB.

Between C and D:

In this documentation

<https://cloud.google.com/load-balancing/docs/https#shared-vpc>

it says that "The global external IP address, the forwarding rule, the target HTTP(S) proxy, and the associated URL map must be defined in the same service project as the backends." and in the statement it says that the MIG are in the service project, so in my opinion the LB components must be in the service project.

👍 ↩ 🚩 upvoted 5 times

🗨️ 👤 **rotorclear** 2 years, 9 months ago

Selected Answer: D

NAT is for outbound while the requirement is to serve external customers who will consume web service. Hence the choice is a LB not NAT

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **soltium** 2 years, 9 months ago

C is the answer.

A B Cloud NAT only handle outbound connection from the VM to internet.

D I'm pretty sure you can't select the service project's MIG as backend when creating LB on the host.

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **AwesomeGCP** 2 years, 9 months ago

Selected Answer: B

B. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **zelck** 2 years, 10 months ago

Selected Answer: D

D is the answer.

<https://cloud.google.com/load-balancing/docs/https#shared-vpc>

While you can create all the load balancing components and backends in the Shared VPC host project, this model does not separate network administration and service development responsibilities.

👍 ↩ 🚩 upvoted 5 times

🗨️ 👤 **rrvv** 2 years, 10 months ago

In shared VPC design, it is possible to create a separate NAT gateway in the service project however as per the best practices, a regional NAT gateway should be created in the host project for each regional subnet/network which is being extended to the attached service projects. Hence I will opt for option B

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **GHOST1985** 2 years, 10 months ago

the requirement says : "while continuing to service external users" , Cloud NAT does not expose service to external users, Cloud NAT is only used for internet outbound
so Answer C is the best Answer

👍 ↩ 🚩 upvoted 3 times

[Load full discussion...](#)

Platform

- > Home
- > Examtopics PRO
- > All Exams
- > Training Courses

