

🔗 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 61 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 61

Topic #: 1

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

A customer wants to deploy a large number of 3-tier web applications on Compute Engine.
How should the customer ensure authenticated network separation between the different tiers of the application?

- A. Run each tier in its own Project, and segregate using Project labels.
- B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.
- C. Run each tier in its own subnet, and use subnet-based firewall rules.
- D. Run each tier with its own VM tags, and use tag-based firewall rules.

[Show Suggested Answer](#)

by [MohitA](#) at *Sept. 2, 2020, 9:07 a.m.*

Comments

Type your comment...

[Submit](#)

🗨️ [genesis3k](#) Highly Voted 4 years, 9 months ago

Answer is B. Keyword is 'authenticated'. Reference below:



"Isolate VMs using service accounts when possible"

"even though it is possible to use tags for target filtering in this manner, we recommend that you use service accounts where

possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped."

<https://cloud.google.com/solutions/best-practices-vpc-design#isolate-vms-service-accounts>

   upvoted 32 times

  **Ric350** 2 years, 3 months ago



Thank you for this great explanation with link to documentation.

   upvoted 1 times

  **gu9singg** 4 years, 4 months ago

document says about subnet isolation

   upvoted 2 times

  **AzureDP900** 2 years, 8 months ago

Agreed with you and B is right

   upvoted 1 times

  **BPzen** Most Recent 8 months ago

Selected Answer: B

Why B is Correct:

Authenticated Separation:

Service accounts are tied to IAM policies and can be used to authenticate requests between tiers. They are access-controlled and cannot be modified dynamically while a VM is running, providing stronger guarantees for isolation. Firewall Rules with Service Accounts:

Google Cloud supports using service accounts as targets for firewall rules. This ensures that traffic can only flow to VMs with specific service accounts, effectively creating authenticated boundaries between tiers.

   upvoted 1 times

  **BPzen** 8 months, 2 weeks ago

Selected Answer: D

VM tags in Google Cloud are a flexible way to categorize and identify virtual machines (VMs) by their function or purpose, such as "frontend," "backend," or "database" for a 3-tier application. By assigning each tier its own tag and applying tag-based firewall rules, the customer can enforce network separation and restrict communication between tiers based on tags. This approach provides authenticated network segmentation by allowing or denying traffic between specific tags, ensuring that only intended communications occur between application tiers.

   upvoted 1 times

  **nairj** 10 months, 2 weeks ago

Ans :C

the question asks for network separation. In case of B, all the tiers are still in the same subnet but are isolated using SA or tags, however, with C, you clearly are separating the network. Hence my answer is C

   upvoted 1 times

  **pico** 1 year, 2 months ago

Selected Answer: C

why the other options are less ideal:

A. Project labels: Project labels are primarily for organizational purposes and don't provide strong network isolation.

B. Service Accounts: While service accounts can be used for authentication, using them alone for network separation can be complex and less effective than subnet-based rules.

D. VM tags: VM tags can be used for filtering in firewall rules, but they don't inherently create network separation.

   upvoted 1 times

  **ArizonaClassics** 1 year, 10 months ago

Run each tier with a different Service Account (SA), and use SA-based firewall rules: Service accounts are primarily designed for authentication and authorization of service-to-service interactions. Using them for network separation is possible but is not their primary use case.



D. Run each tier with its own VM tags, and use tag-based firewall rules: This is the most recommended method for multi-tier applications. VM tags are a straightforward way to identify the role or purpose of a VM (like 'web', 'app', 'database'). When VMs are tagged appropriately, tag-based firewall rules can easily control which tiers can communicate with each other. For example, firewall rules can be set so that only VMs with the 'web' tag can communicate with VMs with the 'app' tag, and so on.

   upvoted 2 times

  **GCBC** 1 year, 11 months ago

B - <https://cloud.google.com/solutions/best-practices-vpc-design#isolate-vms-service-accounts>



   upvoted 2 times

  **riteshahir5815** 2 years, 4 months ago

Selected Answer: C

c is correct answer.

   upvoted 2 times

  **mahi9** 2 years, 5 months ago

Selected Answer: B

SA accounts

   upvoted 1 times

  **AwesomeGCP** 2 years, 9 months ago

Selected Answer: B

B. Run each tier with a different Service Account (SA), and use SA-based firewall rules.

   upvoted 1 times

  **mynk29** 3 years, 5 months ago

"As previously mentioned, you can identify the VMs on a specific subnet by applying a unique network tag or service account to those instances. This allows you to create firewall rules that only apply to the VMs in a subnet—those with the associated network tag or service account. For example, to create a firewall rule that permits all communication between VMs in the same subnet, you can use the following rule configuration on the Firewall rules page:"

B is the right answer

   upvoted 2 times

  **mistryminded** 3 years, 7 months ago

Selected Answer: B


Answer is B - <https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags>

   upvoted 2 times

  **gu9singg** 4 years, 4 months ago


C: is incorrect, we need to authenticate, network rules does not apply and not a recommend best practice from google

   upvoted 2 times

  **gu9singg** 4 years, 4 months ago

C: is incorrect because we need to spend lot of time designing the network topology etc, google recommended practice is to use simple network design with automation in mind, so service account provides those, hence final decision goes to B

   upvoted 2 times

  **gu9singg** 4 years, 4 months ago

Correct answer is B

   upvoted 2 times


  **DebasishLowes** 4 years, 4 months ago


Ans : C

   upvoted 2 times

  **singhjoga** 4 years, 6 months ago

B as per best practices <https://cloud.google.com/solutions/best-practices-vpc-design>

   upvoted 3 times

  **Fellipo** 4 years, 8 months ago

B exists?


   upvoted 1 times

  **[Removed]** 4 years, 9 months ago

Ans - C

https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations#networking_and_security

https://cloud.google.com/solutions/best-practices-vpc-design#addresses_and_subnets

   upvoted 2 times

[Load full discussion...](#)



Platform

> [Home](#)

> [All Exams](#)

> [Examtopics PRO](#)

> [Training Courses](#)

