

[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 87 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 87

Topic #: 1

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

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 the 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 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.
- C. 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.
- 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.

[Show Suggested Answer](#)

by  [Rantu](#) at Oct. 8, 2020, 6:54 p.m.

Comments

Type your comment...

Submit

  **Zuy01** Highly Voted  3 years, 5 months ago

B for sure, u can check this :

<https://cloud.google.com/sql/docs/mysql/sql-proxy#using-a-service-account>

   upvoted 11 times

  **dija123** Most Recent  10 months, 1 week ago

Selected Answer: B

Agree with B

   upvoted 1 times



  **Xoxoo** 1 year, 4 months ago

Selected Answer: B

This approach ensures that only the application frontend can access the data in the MySQL instance, while all other Compute Engine VMs in subnet A and subnet B are restricted from accessing it .

By configuring an ingress firewall rule that allows communication between the frontend's unique service account and the unique service account of the MySQL Compute Engine VM, you can ensure that only authorized users can access your MySQL instance .

   upvoted 2 times

  **GCBC** 1 year, 5 months ago

B Firellas rules using service account is better than tag

   upvoted 2 times

  **AwesomeGCP** 2 years, 3 months ago

Selected Answer: B

B. Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique service account of the mysql ComputeEngine VM on port 3306.

   upvoted 3 times

  **JoseMaria111** 2 years, 4 months ago

B is correct.firellas rules using service account is better than tag based.

https://cloud.google.com/vpc/docs/firewalls#best_practices_for_firewall_rules

   upvoted 2 times

  **mT3** 2 years, 8 months ago

Selected Answer: B

Ans : B

   upvoted 4 times

  **major_querty** 3 years, 2 months ago

why is it not a?

a seems straight forward

The link which Zuy01 provided for answer b states: For this reason, using a service account is the recommended method for production instances NOT running on a Compute Engine instance.

   upvoted 4 times

  **Loved** 2 years, 2 months ago

But answer A says "communication from the src IP range of subnet A"... this rules include all the instances on subnet A, while you have to consider only the frontend

   upvoted 1 times

  **Arturo_Cloud** 2 years, 5 months ago

I agree (A), it is planned to limit a MySQL server in Compute Engine (IaaS) not in Cloud SQL (PaaS), so Networks Tags is the most common and recommended to use. Don't get confused with the services....

   upvoted 2 times

  **DebasishLowes** 3 years, 10 months ago



Ans : B

   upvoted 2 times

  **dtmtor** 3 years, 10 months ago

ans is B

   upvoted 2 times

  **Rantu** 4 years, 3 months ago

B is correct

   upvoted 4 times



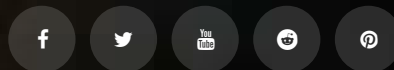
Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses



© 2024 ExamTopics