

[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 202 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 202

Topic #: 1

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

Your Google Cloud organization allows for administrative capabilities to be distributed to each team through provision of a Google Cloud project with Owner role (roles/owner). The organization contains thousands of Google Cloud projects. Security Command Center Premium has surfaced multiple OPEN_MYSQL_PORT findings. You are enforcing the guardrails and need to prevent these types of common misconfigurations.

What should you do?

- A. Create a hierarchical firewall policy configured at the organization to deny all connections from 0.0.0.0/0.
- B. Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges.
- C. Create a Google Cloud Armor security policy to deny traffic from 0.0.0.0/0.
- D. Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0.0.0.0/0 with priority 0.

[Show Suggested Answer](#)

by [K1SMM](#) at Aug. 4, 2023, 1:26 a.m.

Comments

Type your comment...

[Submit](#)

🗄️ 👤 **K1SMM** Highly Voted 👍 1 year, 11 months ago

B - https://cloud.google.com/security-command-center/docs/how-to-remediate-security-health-analytics-findings?hl=pt-br#open_mysql_port

👍 ↩️ 🚩 upvoted 6 times

🗄️ 👤 **dija123** 1 year, 4 months ago

Link in English:

https://cloud.google.com/security-command-center/docs/how-to-remediate-security-health-analytics-findings#open_mysql_port

👍 ↩️ 🚩 upvoted 1 times

🗄️ 👤 **BPzen** Most Recent 🕒 8 months ago

Selected Answer: B

The goal is to enforce guardrails and prevent common misconfigurations, such as exposing MySQL to the public internet, while still allowing legitimate access (e.g., internal or authorized sources). A complete block of all traffic (0.0.0.0/0) at the organizational level may be too restrictive.

Why Option B is a Better Fit
Selective Access:

This policy allows connections to MySQL services only from internal IP ranges (e.g., trusted on-premises networks or other VPCs within the organization).

By restricting access to authorized ranges, you prevent public exposure without fully disabling MySQL functionality.

👍 ↩️ 🚩 upvoted 1 times

🗄️ 👤 **MoAk** 8 months ago

Selected Answer: B

To be honest the Q in itself is crap. Its not specific enough as it does not mention restricting said firewall rules with the SQL port. However having said this, the other answers are crappier so it must be B.

👍 ↩️ 🚩 upvoted 2 times

🗄️ 👤 **Mr_MIXER007** 10 months, 4 weeks ago

Selected Answer: B

Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges

👍 ↩️ 🚩 upvoted 1 times

🗄️ 👤 **3d9563b** 1 year ago

Selected Answer: A

Creating a hierarchical firewall policy at the organization level to deny all connections from 0.0.0.0/0 is the most efficient, scalable, and manageable solution to enforce guardrails and prevent common misconfigurations like open MySQL ports across a large number of projects.

👍 ↩️ 🚩 upvoted 1 times

🗄️ 👤 **b6f53d8** 1 year, 5 months ago

Selected Answer: B

checked with Bard :P

👍 ↩️ 🚩 upvoted 2 times

🗄️ 👤 **Crotofroto** 1 year, 7 months ago

Selected Answer: A

The only option that actually blocks access to the MYSQL port is option A. Other rules should be created with higher priority to avoid infrastructure failures. Option B is not correct because it continues to allow unrestricted connections within the VPC, which may pose a risk of lateral movement.

👍 ↩️ 🚩 upvoted 4 times

🗄️ 👤 **ale_brd_111** 1 year, 5 months ago

Open MySQL port

Category name in the API: OPEN_MYSQL_PORT

Firewall rules that allow any IP address to connect to MySQL ports might expose your MySQL services to attackers. For more information, see VPC firewall rules overview.

The MySQL service ports are:

TCP - 3306

This finding is generated for vulnerable firewall rules, even if you intentionally disable the rules. Active findings for disabled firewall rules alert you to unsafe configurations that will allow undesired traffic if enabled.

To remediate this finding, complete the following steps:

Go to the Firewall page in the Google Cloud console.

Go to Firewall

In the list of firewall rules, click the name of the firewall rule in the finding.

Click edit Edit.



Under Source IP ranges, delete 0.0.0.0/0.

Add specific IP addresses or IP ranges that you want to let connect to the instance.

Add specific protocols and ports you want to open on your instance.

Click Save.

   upvoted 2 times

  **Xoxoo** 1 year, 10 months ago



Selected Answer: B

Your Google Cloud organization allows for administrative capabilities to be distributed to each team through provision of a Google Cloud project with Owner role (roles/owner). The organization contains thousands of Google Cloud projects. Security Command Center Premium has surfaced multiple OPEN_MYSQL_PORT findings. You are enforcing the guardrails and need to prevent these types of common misconfigurations.

What should you do?



- A. Create a hierarchical firewall policy configured at the organization to deny all connections from 0.0.0.0/0.
- B. Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges.
- C. Create a Google Cloud Armor security policy to deny traffic from 0.0.0.0/0.
- D. Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0.0.0.0/0 with priority 0.

   upvoted 2 times

  **arpgaur** 1 year, 10 months ago



we can all use Gen AI to get answers, but sometime even they give a wrong one or when prompted to change, they'll just go with whatever you're saying which is no reliable. Please provide a an official link along with the answer to verify. this does not help anyone.

   upvoted 2 times

  **Xoxoo** 1 year, 10 months ago

I am pretty sure this is more helpful than saying option B is correct or option B makes sense. Instead of calling out you can be more helpful by providing your own link to justify your answer. AI affirm my answers so i am posting here to help others.

   upvoted 1 times

  **Xoxoo** 1 year, 10 months ago

Here's why Option B is the recommended choice:

Hierarchical Firewall Policy: A hierarchical firewall policy set at the organization level allows for centralized control and management of firewall rules across all projects within the organization. This ensures consistent security policies and makes it easier to enforce changes uniformly.

Allow Internal IP Ranges: By configuring the firewall policy to allow connections only from internal IP ranges, you are implementing a "default deny" rule for external traffic, which is a security best practice. This effectively blocks traffic from 0.0.0.0/0 (anywhere), helping to prevent open ports and unauthorized access.

   upvoted 1 times


  **zanhsieh** 7 months, 1 week ago

A: No. Deny all incoming from 0.0.0.0/0 is the firewall default ingress setting.

C: No. Cloud Armor mostly works for L7 ALB, which is not the question asked here. Also it doesn't cover all org projects.

D: No. This will be cumbersome and inefficient for all projects under the org.

   upvoted 1 times

  **Xoxoo** 1 year, 10 months ago

Options A, C, and D have some drawbacks:

Option A (Deny all connections from 0.0.0.0/0) is a strong security measure but could potentially disrupt legitimate traffic if not configured carefully. It's usually recommended to follow the principle of least privilege and explicitly allow

only necessary traffic.

Option C (Create a Google Cloud Armor security policy to deny traffic from 0.0.0.0/0) is more suitable for web application security and might not be the most effective way to prevent open ports like OPEN_MYSQL_PORT.

Option D (Create a firewall rule for each VPC to deny traffic from 0.0.0.0/0 with priority 0) would require creating and managing individual firewall rules for each VPC, which could be cumbersome and less efficient than using a hierarchical firewall policy at the organization level.

👍 ↩ 🚩 upvoted 1 times

🗄 👤 **f983100** 1 year, 7 months ago

That make sense, but how I could control what are the ip internal ranges that each owner uses over his project?

👍 ↩ 🚩 upvoted 1 times

🗄 👤 **Andrei_Z** 1 year, 10 months ago

Selected Answer: B

This question is quite weird, none of the option will prevent this type of misconfiguration

👍 ↩ 🚩 upvoted 3 times

🗄 👤 **cyberpunk21** 1 year, 11 months ago

Selected Answer: B

B is good

👍 ↩ 🚩 upvoted 1 times

🗄 👤 **pfilourenco** 1 year, 11 months ago

Selected Answer: B

B makes sense

👍 ↩ 🚩 upvoted 2 times



Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses

