

🔗 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 191 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 191

Topic #: 1

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

Employees at your company use their personal computers to access your organization's Google Cloud console. You need to ensure that users can only access the Google Cloud console from their corporate-issued devices and verify that they have a valid enterprise certificate.

What should you do?

- A. Implement an Access Policy in BeyondCorp Enterprise to verify the device certificate. Create an access binding with the access policy just created.
- B. Implement a VPC firewall policy. Activate packet inspection and create an allow rule to validate and verify the device certificate.
- C. Implement an organization policy to verify the certificate from the access context.
- D. Implement an Identity and Access Management (IAM) conditional policy to verify the device certificate.

[Show Suggested Answer](#)

by [K1SMM](#) at Aug. 2, 2023, 12:06 p.m.

Comments

Type your comment...

  **Bettoxicity** 10 months ago

Selected Answer: A

BeyondCorp and Access Policies: BeyondCorp is a Google Cloud security framework that focuses on zero-trust principles. Access Policies within BeyondCorp allow you to define granular access controls based on various attributes, including device certificates.

   upvoted 1 times

  **uiuiui** 1 year, 2 months ago

Selected Answer: A

must be A

   upvoted 1 times

  **Xoxoo** 1 year, 4 months ago

Selected Answer: A

Employees at your company use their personal computers to access your organization's Google Cloud console. You need to ensure that users can only access the Google Cloud console from their corporate-issued devices and verify that they have a valid enterprise certificate.

What should you do?

- A. Implement an Access Policy in BeyondCorp Enterprise to verify the device certificate. Create an access binding with the access policy just created.
- B. Implement a VPC firewall policy. Activate packet inspection and create an allow rule to validate and verify the device certificate.
- C. Implement an organization policy to verify the certificate from the access context.
- D. Implement an Identity and Access Management (IAM) conditional policy to verify the device certificate.


   upvoted 1 times

  **ArizonaClassics** 1 year, 5 months ago

A. Implement an Access Policy in BeyondCorp Enterprise to verify the device certificate. Create an access binding with the access policy just created.

This approach is designed to enforce zero-trust access policies, making it a strong fit for the stated needs of only allowing access from corporate-issued devices with valid enterprise certificates.

   upvoted 3 times

  **cyberpunk21** 1 year, 5 months ago

Only option A speaks about device here remaining all false

   upvoted 1 times

  **pfilourenco** 1 year, 5 months ago

Selected Answer: A

A is the correct

   upvoted 2 times

  **K1SMM** 1 year, 5 months ago

A

<https://cloud.google.com/beyondcorp?hl=pt-br>

   upvoted 3 times



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses

