EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 258 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 258
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization is adopting Google Cloud and wants to ensure sensitive resources are only accessible from devices within the internal on-premises corporate network. You must configure Access Context Manager to enforce this requirement. These considerations apply:

• The internal network uses IP ranges 10.100.0.0/16 and 192.168.0.0/16.
• Some employees work remotely but connect securely through a company-managed virtual private network (VPN). The VPN dynamically allocates IP addresses from the pool 172.16.0.0/20.
• Access should be restricted to a specific Google Cloud project that is contained within an existing service perimeter.

What should you do?

A. Create an access level named "Authorized Devices." Utilize the Device Policy attribute to require corporate-managed devices. Apply the access level to the Google Cloud project and instruct all employees to enroll their devices in the organization's management system.

B. Create an access level titled "Internal Network Only." Add a condition with these attributes:
• IP Subnetworks: 10.100.0.0/16, 192.168.0.0/16
• Device Policy: Require OS as Windows or macOS. Apply this access level to the sensitive Google Cloud project.

C. Create an access level titled "Corporate Access." Add a condition with the IP Subnetworks attribute, including the ranges: 10.100.0.0/16, 192.168.0.0/16, 172.16.0.0/20. Assign this access level to a service perimeter encompassing the sensitive project.

D. Create a new IAM role called "InternalAccess. Add the IP ranges 10.100.0.0/16, 192.16.0.0/16, and 172.16.0.0/20 to the role as an IAM condition. Assign this role to IAM groups corresponding to on-premises and VPN users. Grant this role the

necessary permissions on the resource within this sensitive Google Cloud project.

Show Suggested Answer

by yokoyan at *Sept. 6, 2024, 1:26 a.m.*

Comments

Type your comment...

Submit

nah99 8 months ago

Selected Answer: C

https://cloud.google.com/access-context-manager/docs/overview#ip-address

upvoted 2 times

BondleB 8 months, 4 weeks ago

Selected Answer: C

The recommended approach is to configure Access Context Manager to create access levels incorporating the specified IP ranges (10.100.0.0/16, 192.168.0.0/16, and 172.16.0.0/20) and apply this access level to the existing service perimeter containing the sensitive resources.
This method leverages Google Cloud's built-in security features to enforce network-based access controls effectively and provides better security and compliance for the sensitive resources.

upvoted 2 times

yokoyan 10 months, 3 weeks ago

Selected Answer: C

I think it's C.

upvoted 1 times