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 44 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 44

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your company is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee's password has been compromised.

What should you do?

A. Enforce 2-factor authentication in GSuite for all users.

B. Configure Cloud Identity-Aware Proxy for the App Engine Application.

C. Provision user passwords using GSuite Password Sync.

D. Configure Cloud VPN between your private network and GCP.

Show Suggested Answer

by rafaelc at *March 14, 2020, 9:53 a.m.*

Comments

Type your comment...

Submit

⊟ rafaelc Highly Voted 5 years, 4 months ago

A. Enforce 2-factor authentication in GSuite for all users.

upvoted 22 times

lolanczos Most Recent 5 months ago

Selected Answer: B

B is correct

Cloud Identity-Aware Proxy (IAP) enforces identity-based access controls directly at the application layer, ensuring that only authenticated and authorized users can access the App Engine application. It adds an additional security layer independent of the user’s credentials, thereby protecting the application even if an employee’s password is compromised. A is not sufficient because enforcing 2FA only protects the authentication process and does not provide the granular, context-aware access control that IAP offers.

upvoted 2 times

anciaosinclinado 4 months, 3 weeks ago

But if the user's password is compromised and there is no 2FA configured for that account, an attacker would be able to authenticate even if the application uses IAP.

upvoted 2 times

Rakesh21 6 months ago

Selected Answer: A

Default IAP Configuration: By default, IAP requires users to be authenticated with Google accounts, but this authentication might only involve a username and password unless 2FA is specifically enforced for those accounts by the organization's security policies in Google Workspace or Cloud Identity.

upvoted 1 times

coompiler 9 months, 1 week ago

Selected Answer: B

I go with B. IAP is zero trust and context aware

upvoted 1 times

coompiler 9 months, 1 week ago

I go with B. IAP is zero trust and context aware

upvoted 1 times

PankajKapse 10 months, 1 week ago

Selected Answer: B

I also feel, it's B. As even if password is compromised, we can block based on IP ranges, geolocation, etc

upvoted 1 times

Oujay 1 year, 1 month ago

Selected Answer: B

A Cloud VPN creates a secure tunnel between your network and GCP, but it wouldn't restrict access based on individual user identities.

upvoted 2 times

Oujay 1 year, 1 month ago

2FA adds an extra layer of security, but if an external user has both the password and the second factor (e.g., a verification code), they might still gain access.
So my answer is B. All external users will be blocked with the right authentication or not

upvoted 1 times

dbf0a72 1 year, 6 months ago

Selected Answer: A

A is the answer.

upvoted 1 times

raj117 2 years ago

Right Answer is A

upvoted 2 times

SMB2022 2 years ago

Correct Answer A

upvoted 2 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: A

A is the answer.

upvoted 3 times

sudarchary 3 years, 5 months ago

Selected Answer: A

https://support.google.com/a/answer/175197?hl=en

upvoted 2 times

Jane111 4 years, 3 months ago

Shouldn't it be
B. Configure Cloud Identity-Aware Proxy for the App Engine Application.
identity based app access

upvoted 4 times

> **[Removed]** 2 years ago
>
> I was thinking the same thing. Turns out IAP ensures security by enforcing 2FA. So at the end of the day, 2FA is the real solution.
> 2FA without IAP would still address the risk. IAP without 2FA might not.
> https://cloud.google.com/iap/docs/configuring-reauth#supported_reauthentication_methods
>
> upvoted 2 times

desertlotus1211 4 years, 4 months ago

The key is external user. Best practice is to have internal users/datacenter connect via VPN for security purpose, correct? External users will try to connect via Internet - they still cannot reach the app engine even if they have a users' password because a VPN connection is need to reach the resource. MA will work IF the external user has VPN access... But I think D is what they're looking for based on the question....

upvoted 3 times

> **mynk29** 3 years, 5 months ago
>
> Agree but there is no mention that external user doesnt have internal network access too. A is better option as it covers both scenarios.
>
> upvoted 2 times

DebasishLowes 4 years, 4 months ago

Ans : A. When passwords is compromised, enforcing 2 factor authentication is the best way to prevent non authorized users.

upvoted 2 times

soukumar369 4 years, 7 months ago

Enforcing 2-factor authentication can save an employee's password has been compromised

upvoted 2 times

Load full discussion...