≡ MENU 🔍

← 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 80 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 80

Topic #: 1

[All Professional Cloud Security Engineer Questions]

An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.
Your team wants to avoid exposing the application directly on the internet and wants to deny traffic from a specific list of malicious IP addresses.
Which solution should your team implement to meet these requirements?

    A. Cloud Armor

    B. Network Load Balancing

    C. SSL Proxy Load Balancing

    D. NAT Gateway

Show Suggested Answer

by 👤 **mlyu** at *Sept. 12, 2020, 2:42 p.m.*

Comments

Type your comment...

Submit

☐ 👤 **DebasishLowes** `Highly Voted 👍` 2 years, 10 months ago

Ans : A

👍 ↩ 🚩 upvoted 8 times

☐ 👤 **BillBaits** 2 years, 2 months ago

Think so

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **Appsec977** `Most Recent ⏱` 8 months, 1 week ago

`Selected Answer: A`

We can block the specific IPs in Cloud armor using simple rules or can use advanced rules using Common Expression Language(CEL).

👍 ↩ 🚩 upvoted 4 times

☐ 👤 **shayke** 1 year, 1 month ago

`Selected Answer: A`

A Is the only ans because you are asked to limit access by IP and CA is the only option

👍 ↩ 🚩 upvoted 2 times

☐ 👤 **AzureDP900** 1 year, 2 months ago

This is straight forward question, A is right

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **AwesomeGCP** 1 year, 3 months ago

`Selected Answer: A`

A. Cloud Armor

👍 ↩ 🚩 upvoted 2 times

☐ 👤 **cloudprincipal** 1 year, 7 months ago

`Selected Answer: A`

https://cloud.google.com/armor/docs/security-policy-overview#edge-security

👍 ↩ 🚩 upvoted 2 times

☐ 👤 **mlyu** 3 years, 4 months ago

Definitly B

👍 ↩ 🚩 upvoted 2 times

☐ 👤 **ownez** 3 years, 4 months ago

Should be A? Cloud armor can deny traffic by defining IP addresses list rule and to avoid exposing the application directly on the internet.

While Network LB is using Google Cloud firewalls to control or filter access to the backend VMs.

Answer is A.

👍 ↩ 🚩 upvoted 5 times

☐ 👤 **mlyu** 3 years, 3 months ago

you are correct. Answer is A
The Cloud armor able to directed user traffic to an external HTTP(S) load balancer enters the PoP closest to the user in Premium Tier.
https://cloud.google.com/armor/docs/security-policy-overview#edge-security

👍 ↩ 🚩 upvoted 5 times