

[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 6 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 6

Topic #: 1

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

A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's internal compliance requirements dictate that end- user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection.

Which product should be used to meet these requirements?


- A. Cloud Armor
- B. VPC Firewall Rules
- C. Cloud Identity and Access Management
- D. Cloud CDN

[Show Suggested Answer](#)

by  **KILLMAD** at *March 9, 2020, 11 a.m.*

Comments

[Submit](#)

 **KILLMAD** Highly Voted  5 years, 4 months ago

Answer is A

   upvoted 18 times

 **juanmacoelloccloudsecarch** Most Recent  1 week, 3 days ago

Selected Answer: A

This question is asking us about "Web application" ... You have to think directly in the WAF ... So first thing is Cloud Armor...

If you keep reading this talk about SYN, That's a TCP Protocol from L4 and VPC Rules are L3 (IP not transport layer)...

A.

   upvoted 1 times

 **The_Snobby** 2 months ago

Selected Answer: B

C and D are wrong. So its A or B. standard DDoS is fulfilled for both, but for A you need a load-balancer and it costs additional. In the question it is only 3-tier, which does not need a loadbalancer and it is specifically mentioned that the do not need the advanced security, which would come with cloud armor at additional costs. That only leaves B.

   upvoted 1 times

 **Subrat674** 2 months, 3 weeks ago

Selected Answer: A

Answer is A.

   upvoted 1 times

 **Astro_123** 3 months, 2 weeks ago

Selected Answer: B

Answer is B

   upvoted 1 times

 **zanhsieh** 7 months, 1 week ago

Selected Answer: A

I will still stick with A since Cloud Armor supports regional internal application load balancer:

<https://cloud.google.com/load-balancing/docs/l7-internal#backend-features>

<https://cloud.google.com/load-balancing/docs/l7-internal/int-https-lb-tf-examples>

Also the question does not ask for cross region, Cloud Armor should be an easier and safer bet.

   upvoted 1 times

 **BPzen** 8 months, 2 weeks ago

Selected Answer: A

Cloud Armor: This service is specifically designed for web application and API protection. It allows you to configure rules based on IP addresses (CIDR ranges), and it includes built-in DDoS protection, including SYN flood protection. This directly addresses the customer's requirements.

Here's why the other options are not the best fit:

B. VPC Firewall Rules: These are primarily for controlling traffic within your VPC network. While you can restrict traffic based on IP addresses, they don't offer the advanced DDoS protection capabilities of Cloud Armor.

   upvoted 1 times

 **3d9563b** 1 year ago

Selected Answer: B

VPC Firewall Rules will allow you to control access based on CIDR ranges, ensuring that only traffic from the specified IP addresses is permitted. Additionally, GCP provides built-in SYN flood protection as part of its infrastructure. This solution aligns with both the internal compliance requirements and the acceptance of the risk regarding SYN flood attacks.

   upvoted 2 times

 **alilikpo** 1 year, 1 month ago

Selected Answer: B

While Cloud Armor offers advanced DDoS protection, it's not the most suitable choice for restricting access based on known good CIDRs in this scenario. Cloud Armor excels at mitigating volumetric DDoS attacks like SYN floods, but its access control mechanisms aren't specifically designed for CIDR-based whitelisting.

   upvoted 4 times

 **charlesdeng** 1 year, 3 months ago

Selected Answer: B

For internal web application, it shall be used by VPC Firewall Rules

   upvoted 2 times

 **nnandher** 1 year, 9 months ago

— **ppandey96** 2 years, 4 months ago

Can Cloud Armor be used for INTERNAL Applications ? I think - NO, as it is used for External attacks-
so Answer should be - B VPC Firewall Rules. Verified from ChatGPT3.5

👍 ↩ 🚩 upvoted 4 times

🗄 **mildi** 2 years ago

Answer A if no Load balancer used

👍 ↩ 🚩 upvoted 1 times

🗄 **mildi** 2 years ago

I mean B if no load balancer used

👍 ↩ 🚩 upvoted 1 times

🗄 **pfilourenco** 2 years, 1 month ago

Selected Answer: A

Answer is A

👍 ↩ 🚩 upvoted 1 times

🗄 **ppandey96** 2 years, 4 months ago

Selected Answer: A

<https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps>

👍 ↩ 🚩 upvoted 1 times

🗄 **civilizador** 2 years, 5 months ago

<https://cloud.google.com/files/GCPDDoSprotection-04122016.pdf>

It doesn't say a word about cloud Armor in the context of DDoS attacks because it is not the main feature of Cloud Armor. In the DDoS mitigation best practices only mentioned Load Balancer, Firewall rules and CDN. So I don't know if it is either Firewall rules or CDN. Most likely Firewall rules since CDN doesn't directly prevent the attack more like distributes it through multiple global endpoints.

Little bit tricky question.

👍 ↩ 🚩 upvoted 1 times

🗄 **civilizador** 2 years, 1 month ago

The question clearly indicates that request should be allowed only if originating from a specific CIDR so the answer is a firewall rules

👍 ↩ 🚩 upvoted 2 times

🗄 **shetniel** 2 years, 5 months ago

It is an internal web application and they need to allow access only for user traffic originated from a specific CIDR. They are fine with just default SYN flood protection. This can very well be handled by a VPC firewall rule.

👍 ↩ 🚩 upvoted 4 times

🗄 **alestrix** 2 years, 6 months ago

Selected Answer: B

For CIDR check the firewall is sufficient and SYN flood protection is already given by the regular load balancer in front of the service. Armor gives much more than just SYN flood protection and given the statement "their application will only have SYN flood DDoS protection" this is another vote against Armor.

👍 ↩ 🚩 upvoted 2 times

🗄 **gcpengineer** 2 years, 2 months ago

the External Load Balancer (LB) does not provide built-in protection against SYN flood DDoS attacks

👍 ↩ 🚩 upvoted 1 times

[Load full discussion...](#)



Platform

> Home

> All Exams

