

[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 130 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 130

Topic #: 1

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

You plan to use a Google Cloud Armor policy to prevent common attacks such as cross-site scripting (XSS) and SQL injection (SQLi) from reaching your web application's backend. What are two requirements for using Google Cloud Armor security policies? (Choose two.)

- A. The load balancer must be an external SSL proxy load balancer.
- B. Google Cloud Armor Policy rules can only match on Layer 7 (L7) attributes.
- C. The load balancer must use the Premium Network Service Tier.
- D. The backend service's load balancing scheme must be EXTERNAL.
- E. The load balancer must be an external HTTP(S) load balancer.

[Show Suggested Answer](#)

by  [Tabayashi](#) at April 29, 2022, 3:30 a.m.

Comments

[Submit](#)

  [i_am_robot](#) 11 months, 3 weeks ago

Selected Answer: DE

Here's the reasoning:

D is correct because according to search result , one of the requirements for using Google Cloud Armor security policies is that "The backend service's load balancing scheme must be EXTERNAL, EXTERNAL_MANAGED, or INTERNAL_MANAGED." The EXTERNAL scheme is specifically mentioned in the answer option.



E is correct because Google Cloud Armor is primarily designed to work with HTTP(S) load balancers. This is supported by multiple search results, including which states that Google Cloud Armor security policies protect "Global external Application Load Balancer (HTTP/HTTPS)" among others.

   upvoted 1 times

  **LaithTech** 11 months, 3 weeks ago

Google Cloud Armor is only supported with the Premium Network Service Tier. The Standard Tier does not support Google Cloud Armor features.

   upvoted 1 times

  **nah99** 8 months, 1 week ago

This says otherwise

<https://cloud.google.com/armor/docs/security-policy-overview#requirements>

   upvoted 1 times

  **Betotoxicity** 1 year, 4 months ago


Selected Answer: BE

BE

B: Google Cloud Armor operates at Layer 7 (application layer) of the OSI model. Its security policies inspect incoming HTTP(S) requests and can match on various L7 attributes like request headers, body content, and URI paths. This allows you to define rules that block attacks like XSS and SQLi based on their specific characteristics.

Why not C: The load balancing scheme of the backend service (internal or external) doesn't impact Cloud Armor's operation. Cloud Armor focuses on filtering traffic at the external load balancer level.

   upvoted 1 times

  **aygitci** 1 year, 9 months ago

Why not B?

   upvoted 2 times

  **Xoxoo** 1 year, 10 months ago

Selected Answer: DE

To use Google Cloud Armor security policies to prevent common attacks such as cross-site scripting (XSS) and SQL injection (SQLi) from reaching your web application's backend, you need to meet the following requirements :

- 1) The load balancer must be a global external Application Load Balancer, a classic Application Load Balancer, a regional external Application Load Balancer, or an external proxy Network Load Balancer .
- 2) The backend service's load balancing scheme must be EXTERNAL, or EXTERNAL_MANAGED if you are using either a global external Application Load Balancer or a regional external Application Load Balancer .

   upvoted 1 times

  **[Removed]** 2 years ago

Selected Answer: DE

"D", "E"

As others noted in the comments, "A", "D" and "E" all meet the minimum requirements for setting up Cloud Armor. However part of the question is having WAF functionality which is not available for External SSL Proxy LBs (A) (no checkmark under external proxy lb column for WAF row).

This which leaves us with D and E only.

References:

<https://cloud.google.com/armor/docs/security-policy-overview#requirements>

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

   upvoted 1 times

  **gcpengineer** 2 years, 2 months ago




Now we can manage also network load balancer

   upvoted 1 times

  **gcpengineer** 2 years, 2 months ago

Selected Answer: DE

DE is the ans

   upvoted 1 times

🗄️ 👤 **AzureDP900** 2 years, 8 months ago

D,E is most appropriate in this case
D. The backend service's load balancing scheme must be EXTERNAL.
E. The load balancer must be an external HTTP(S) load balancer.

👍 ↩️ 🚩 upvoted 2 times

🗄️ 👤 **soltium** 2 years, 9 months ago

Selected Answer: DE

DE.
Well technically you can use EXTERNAL_MANAGED scheme too.

👍 ↩️ 🚩 upvoted 1 times

🗄️ 👤 **AwesomeGCP** 2 years, 9 months ago

Selected Answer: DE

D. The backend service's load balancing scheme must be EXTERNAL.
E. The load balancer must be an external HTTP(S) load balancer.

👍 ↩️ 🚩 upvoted 1 times

🗄️ 👤 **Jeanphi72** 2 years, 11 months ago

Selected Answer: DE

<https://cloud.google.com/armor/docs/security-policy-overview#requirements> says:
The backend service's load balancing scheme must be EXTERNAL, or EXTERNAL_MANAGED *** if you are using global external HTTP(S) load balancer ***.

Thus D and E fit (A could fit if a suggestion like The backend service's load balancing scheme must ** NOT ** be EXTERNAL

👍 ↩️ 🚩 upvoted 2 times

🗄️ 👤 **piyush_1982** 2 years, 12 months ago

I am not sure if there is some mistake in the question or in the options given.

<https://cloud.google.com/armor/docs/security-policy-overview#requirements>

As per the link above, below are the requirements for using Google Cloud Armor security policies:

1. The load balancer must be a global external HTTP(S) load balancer, global external HTTP(S) load balancer (classic), external TCP proxy load balancer, or external SSL proxy load balancer.
2. The backend service's load balancing scheme must be EXTERNAL, or EXTERNAL_MANAGED if you are using a global external HTTP(S) load balancer.
3. The backend service's protocol must be one of HTTP, HTTPS, HTTP/2, TCP, or SSL.

The correct answer seems to be A D and E.

A. The load balancer must be an external SSL proxy load balancer. (external SSL proxy load balancer is one of the load balancing options listed in the link)
D. The backend service's load balancing scheme must be EXTERNAL. (or EXTERNAL_MANAGED)
E. The load balancer must be an external HTTP(S) load balancer. (Also one of the options listed)

👍 ↩️ 🚩 upvoted 3 times

🗄️ 👤 **zellick** 2 years, 10 months ago

Security policy for A does not block XSS and SQLi which is at layer 7.
<https://cloud.google.com/armor/docs/security-policy-overview#policy-types>

👍 ↩️ 🚩 upvoted 5 times

🗄️ 👤 **TNT87** 2 years, 3 months ago

Not true....Security policy overview

bookmark_border

Google Cloud Armor security policies protect your application by providing Layer 7 filtering and by scrubbing incoming requests for common web attacks or other Layer 7 attributes to potentially block traffic before it reaches your load balanced backend services or backend buckets. Each security policy is made up of a set of rules that filter traffic based on conditions such as an incoming request's IP address, IP range, region code, or request headers.

Google Cloud Armor security policies are available only for backend services of global external HTTP(S) load balancers, global external HTTP(S) load balancer (classic)s, external TCP proxy load balancers, or external SSL proxy load balancers. The load balancer can be in Premium Tier or Standard Tier.
<https://cloud.google.com/armor/docs/security-policy-overview> . A, D,E are correct

👍 ↩️ 🚩 upvoted 1 times

🗄️ 👤 **[Removed]** 2 years ago

If you look at the table here, you'll see that the row that has "WAF" (which is what you need here for web application firewall) is unchecked under the External Proxy LB column. This disqualifies "A" from the answer and leaves us with "D" and "E" only.

Reference:

<https://cloud.google.com/armor/docs/security-policy-overview#expandable-1>

So good catch piyush_1982 and zelck !

👍 🔄 🚩 upvoted 1 times

📄 👤 **nacying** 3 years, 1 month ago

Selected Answer: DE

These are the requirements for using Google Cloud Armor security policies:

The load balancer must be an external HTTP(S) load balancer, TCP proxy load balancer, or SSL proxy load balancer.

The backend service's load balancing scheme must be EXTERNAL.

The backend service's protocol must be one of HTTP, HTTPS, HTTP/2, TCP, or SSL.

<https://cloud.google.com/armor/docs/security-policy-overview>

👍 🔄 🚩 upvoted 1 times

📄 👤 **cloudprincipal** 3 years, 1 month ago

Selected Answer: DE

DE

Requirements

These are the requirements for using Google Cloud Armor security policies:

* The load balancer must be an external HTTP(S) load balancer, TCP proxy load balancer, or SSL proxy load balancer.

* The backend service's load balancing scheme must be EXTERNAL.

* The backend service's protocol must be one of HTTP, HTTPS, HTTP/2, TCP, or SSL.

See <https://cloud.google.com/armor/docs/security-policy-overview#requirements>

👍 🔄 🚩 upvoted 3 times

📄 👤 **szl0144** 3 years, 2 months ago

Google Cloud Armor security policies are sets of rules that match on attributes from Layer 3 to Layer 7 to protect externally facing applications or services. Each rule is evaluated with respect to incoming traffic.

I choose DE

👍 🔄 🚩 upvoted 1 times

📄 👤 **ExamQnA** 3 years, 2 months ago

Ans:D,E

<https://cloud.google.com/armor/docs/security-policy-overview>

Relevant extracts:

1. Google Cloud Armor security policies enable you to rate-limit or redirect requests to your HTTP(S) Load Balancing, TCP Proxy Load Balancing, or SSL Proxy Load Balancing ...

2. Google Cloud Armor security policies are sets of rules that match on attributes from Layer 3 to Layer 7 to protect externally facing applications or services...

3. The load balancer can be in Premium Tier or Standard Tier.

👍 🔄 🚩 upvoted 3 times

[Load full discussion...](#)



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses

