Google Discussions

EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 189 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 189
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your application is deployed as a highly available, cross-region solution behind a global external HTTP(S) load balancer. You notice significant spikes in traffic from multiple IP addresses, but it is unknown whether the IPs are malicious. You are concerned about your application's availability. You want to limit traffic from these clients over a specified time interval.

What should you do?

A. Configure a throttle action by using Google Cloud Armor to limit the number of requests per client over a specified time interval.

B. Configure a rate_based_ban action by using Google Cloud Armor and set the ban_duration_sec parameter to the specified lime interval.

C. Configure a firewall rule in your VPC to throttle traffic from the identified IP addresses.

D. Configure a deny action by using Google Cloud Armor to deny the clients that issued too many requests over the specified time interval.

Show Suggested Answer

by K1SMM at *Aug. 2, 2023, 12:01 p.m.*

Comments

Type your comment...

Submit

Xoxoo 10 months, 1 week ago

Selected Answer: A

To limit traffic from the identified IP addresses over a specified time interval, you should configure a throttle action by using Google Cloud Armor. This will limit the number of requests per client over a specified time interval, which can help prevent your application from being overwhelmed by traffic spikes.

Option B is not recommended because it would ban the clients that issue too many requests over the specified time interval, which might not be desirable if the clients are legitimate.

Option C is not recommended because it would throttle traffic from all IP addresses that match the firewall rule, which might not be desirable if some of the IP addresses are legitimate.

Option D is not recommended because it would deny the clients that issue too many requests over the specified time interval, which might not be desirable if the clients are legitimate.

Therefore, Option A is the most appropriate choice for limiting traffic from multiple IP addresses over a specified time interval.

upvoted 2 times

ArizonaClassics 11 months ago

When dealing with potential DDoS attacks or unexpected spikes in traffic, it's essential to handle the situation carefully to maintain the availability of your application. Here are the options you have:

A. Configure a throttle action by using Google Cloud Armor: Google Cloud Armor allows you to define security policies that can throttle clients based on the number of incoming requests over a certain time period. This ensures that legitimate users are not completely blocked while also preventing any one client from overloading the system.

upvoted 1 times

cyberpunk21 11 months, 1 week ago

Selected Answer: A

All can be done but option A is correct cuz a sentence "number of requests per client."

upvoted 2 times

a190d62 12 months ago

Selected Answer: A

A
you want to limit, not ban traffic

https://cloud.google.com/armor/docs/rate-limiting-overview#throttle-traffic

upvoted 4 times

K1SMM 12 months ago

A
https://cloud.google.com/blog/products/identity-security/announcing-new-cloud-armor-rate-limiting-adaptive-protection-and-bot-defense

upvoted 1 times