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 262 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 262

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your organization hosts a sensitive web application in Google Cloud. To protect the web application, you've set up a virtual private cloud (VPC) with dedicated subnets for the application's frontend and backend components. You must implement security controls to restrict incoming traffic, protect against web-based attacks, and monitor internal traffic. What should you do?

A. Configure Cloud Firewall to permit allow-listed traffic only, deploy Google Cloud Armor with predefined rules for blocking common web attacks, and deploy Cloud Intrusion Detection System (IDS) to detect internal traffic anomalies.

B. Configure Google Cloud Armor to allow incoming connections, configure DNS Security Extensions (DNSSEC) on Cloud DNS to secure against common web attacks, and deploy Cloud Intrusion Detection System (Cloud IDS) to detect internal traffic anomalies.

C. Configure Cloud Intrusion Detection System (Cloud IDS) to monitor incoming connections, deploy Identity-Aware Proxy (IAP) to block common web attacks, and deploy Google Cloud Armor to detect internal traffic anomalies.

D. Configure Cloud DNS to secure incoming traffic, deploy Cloud Intrusion Detection System (Cloud IDS) to detect common web attacks, and deploy Google Cloud Armor to detect internal traffic anomalies.

Show Suggested Answer

by yokoyan at *Sept. 6, 2024, 1:29 a.m.*

Comments

Type your comment...

Submit

Pime13 7 months, 3 weeks ago

Selected Answer: A

Here's why:

Cloud Firewall: By configuring the firewall to permit only allow-listed traffic, you can restrict incoming traffic to only trusted sources, enhancing security.
Google Cloud Armor: This service provides protection against common web-based attacks such as DDoS and SQL injection by using predefined rules.
Cloud Intrusion Detection System (IDS): Deploying IDS helps in monitoring internal traffic for any anomalies, ensuring that any suspicious activity within the VPC is detected and addressed promptly.
This combination of services provides a comprehensive security posture for your sensitive web application, addressing both external and internal threats.

upvoted 1 times

MoAk 8 months, 1 week ago

Selected Answer: A

A is good.

upvoted 1 times

yokoyan 10 months, 3 weeks ago

Selected Answer: A

I think it's A.

upvoted 2 times