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 111 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 111

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your company requires the security and network engineering teams to identify all network anomalies within and across VPCs, internal traffic from VMs to VMs, traffic between end locations on the internet and VMs, and traffic between VMs to Google Cloud services in production. Which method should you use?

A. Define an organization policy constraint.

B. Configure packet mirroring policies.

C. Enable VPC Flow Logs on the subnet.

D. Monitor and analyze Cloud Audit Logs.

Show Suggested Answer

by Tabayashi at *April 29, 2022, 3:16 a.m.*

Comments

Type your comment...

Submit

Tabayashi Highly Voted 2 years, 9 months ago

I think the answer is (C).

VPC Flow Logs samples each VM's TCP, UDP, ICMP, ESP, and GRE flows. Both inbound and outbound flows are sampled. These flows can be between the VM and another VM, a host in your on-premises data center, a Google service, or a host on the internet.
https://cloud.google.com/vpc/docs/flow-logs

upvoted 13 times

hybridpro Highly Voted 2 years, 7 months ago

B should be the answer. For detecting network anomalies, you need to have payload and header data as well to be effective. Besides C is saying to enable VPC flow logs on a subnet which won't serve our purpose either.

upvoted 8 times

dija123 Most Recent 10 months, 4 weeks ago

Selected Answer: B

Backet mirroring policies allow you to mirror all traffic passing through a specific network interface or VPC route to a designated destination (e.g., another VM, a Cloud Storage bucket). This captured traffic can then be analyzed by security and network engineers using tools like Suricata or Security Command Center for advanced anomaly detection. This approach provides the necessary level of detail and flexibility for identifying anomalies across all the mentioned traffic types

upvoted 1 times

b6f53d8 1 year ago

C is only for subnet, and we need control in many VPCs, so I prefer B

upvoted 1 times

sebG35 1 year, 1 month ago

The answer is C. The needs is identify all network anomalies within and across VPCs, internal traffic from VMs to VMs ...

B- Does not meet all needs. It is limited to the VM and don't cover the needs : across VPCs
https://cloud.google.com/vpc/docs/packet-mirroring?hl=en

C- Cover all needs
https://cloud.google.com/vpc/docs/flow-logs?hl=en

upvoted 1 times

tifo16 2 years, 1 month ago

https://cloud.google.com/vpc/docs/packet-mirroring#enterprise_security

Security and network engineering teams must ensure that they are catching all anomalies and threats that might indicate security breaches and intrusions. They mirror all traffic so that they can complete a comprehensive inspection of suspicious flows. Because attacks can span multiple packets, security teams must be able to get all packets for each flow.

upvoted 3 times

> **tifo16** 2 years, 1 month ago
>
> Should be B
>
> upvoted 2 times

Rightsaidfred 2 years, 2 months ago

As it is a close tie and ambiguity between B&C, I would say it is C - VPC Flow Logs in this instance, as Question 121 is focusing more on Packet Mirroring with the IDS Use Case.

upvoted 2 times

marmar11111 2 years, 2 months ago

Selected Answer: B

Should be B

upvoted 3 times

hcnh 2 years, 2 months ago

Selected Answer: C

C is the answer as B has the limitation against question

The mirroring happens on the virtual machine (VM) instances, not on the network. Consequently, Packet Mirroring consumes additional bandwidth on the VMs.

upvoted 3 times

AwesomeGCP 2 years, 3 months ago

Selected Answer: B

B. Configure packet mirroring policies.

upvoted 5 times

zellck 2 years, 4 months ago

Selected Answer: B

B is the answer.

https://cloud.google.com/vpc/docs/packet-mirroring#enterprise_security
Security and network engineering teams must ensure that they are catching all anomalies and threats that might indicate security breaches and intrusions. They mirror all traffic so that they can complete a comprehensive inspection of suspicious flows.

upvoted 3 times

AzureDP900 2 years, 2 months ago

Agree with B

upvoted 2 times

GHOST1985 2 years, 4 months ago

Selected Answer: B

100% Answer B: Anomalies means packet miroiring
https://cloud.google.com/vpc/docs/packet-mirroring#enterprise_security
"Packet Mirroring is useful when you need to monitor and analyze your security status. It exports all traffic, not only the traffic between sampling periods. For example, you can use security software that analyzes mirrored traffic to detect all threats or anomalies. Additionally, you can inspect the full traffic flow to detect application performance issues. For more information, see the example use cases."
https://cloud.google.com/vpc/docs/packet-mirroring

upvoted 2 times

tangac 2 years, 4 months ago

Selected Answer: C

First you can use VPC flow log at a subnet level : https://cloud.google.com/vpc/docs/using-flow-logs
Then VPC Flow Log main feature is to collect logs that can be used for network monitoring, forensics, real-time security analysis, and expense optimization.

upvoted 1 times

jvkubjg 2 years, 5 months ago

Selected Answer: B

Anomalies -> Packet Mirroring

upvoted 1 times

mikesp 2 years, 7 months ago

Selected Answer: C

VPC Flow Logs also helps you perform network forensics when investigating suspicious behavior such as traffic from access from abnormal sources or unexpected volumes of data migration

upvoted 3 times