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 174 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 174
Topic #: 1
[All Professional Cloud Security Engineer Questions]

You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your VPCs based on network logs. However, you want to explore your environment using network payloads and headers. Which Google Cloud product should you use?

A. Cloud IDS

B. VPC Service Controls logs

C. VPC Flow Logs

D. Google Cloud Armor

E. Packet Mirroring

Show Suggested Answer

by Random_Mane at *Sept. 5, 2022, 8:31 p.m.*

### Comments

Type your comment...

Submit

zellck Highly Voted 2 years, 10 months ago

Selected Answer: E

E is the answer.

https://cloud.google.com/vpc/docs/packet-mirroring
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

upvoted 10 times

**kalyan_krishna742020** Highly Voted 2 years, 7 months ago

It should be A..
Cloud IDS inspects not only the IP header of the packet, but also the payload.
https://cloud.google.com/blog/products/identity-security/how-google-cloud-ids-helps-detect-advanced-network-threats

upvoted 8 times

**JohnDohertyDoe** Most Recent 7 months ago

Selected Answer: A

Both A and E would work, but in this case I believe Cloud IDS is a better fit as it is monitor and prevent network anomalies.

upvoted 1 times

**Pime13** 7 months, 2 weeks ago

Selected Answer: E

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

Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers. The capture can be configured for both egress and ingress traffic, only ingress traffic, or only egress traffic.

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

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.

upvoted 1 times

**MoAk** 8 months, 1 week ago

Answer previously would have been E however, I believe this now should be Answer A - Cloud IDS

upvoted 2 times

**Bettoxicity** 1 year, 3 months ago

Selected Answer: E

E.

Packet Mirroring allows you to replicate network traffic flowing through your VPCs to a designated destination. This destination can be a dedicated instance or a network analysis tool. With full packet capture, you can inspect the contents of network payloads and headers, providing a deeper level of network traffic analysis compared to just flow logs.

upvoted 1 times

**desertlotus1211** 1 year, 10 months ago

Answer is A:
It askes for 'Google Cloud Product'. Cloud IDS includes packet mirroring and built with Palo Alto threat detection.

https://www.happtiq.com/cloud-ids/

After an endpoint has been specified, traffic from specific instances is cloned by setting up a packet mirroring policy. All the data from the traffic along with packet data, payloads, and headers is forwarded to Cloud IDS for examination.

upvoted 2 times

**cyberpunk21** 1 year, 11 months ago

Selected Answer: E

E is the answer

upvoted 1 times

**desertlotus1211** 1 year, 10 months ago

Answer is A:
It askes for 'Google Cloud Product'. Cloud IDS includes packet mirroring and built with Palo Alto threat detection.

https://www.happtiq.com/cloud-ids/

After an endpoint has been specified, traffic from specific instances is cloned by setting up a packet mirroring policy. All

the data from the traffic along with packet data, payloads, and headers is forwarded to Cloud IDS for examination.

upvoted 1 times

**gcpengineer** 2 years, 2 months ago

Selected Answer: A

cloud IDS is based on packet mirroring and asked for product to analyse. so A is the ans

upvoted 3 times

**AzureDP900** 2 years, 8 months ago

E

Packet Mirroring captures all traffic and packet data, including payloads and headers. The capture can be configured for both egress and ingress traffic, only ingress traffic, or only egress traffic.

upvoted 3 times

**hello_gcp_devops** 2 years, 9 months ago

Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers. The capture can be configured for both egress and ingress traffic, only ingress traffic, or only egress traffic.

upvoted 1 times

**hello_gcp_devops** 2 years, 9 months ago

E is the answer

upvoted 2 times

**Random_Mane** 2 years, 10 months ago

Selected Answer: E

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

upvoted 3 times