PROFESSIONAL-CLOUD-SECURITY-ENGINEER Q&As

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass2lead.com/professional-cloud-security-engineer.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

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.

Correct Answer: B

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.

QUESTION 2

Your company uses Google Cloud and has publicly exposed network assets. You want to discover the assets and perform a security audit on these assets by using a software tool in the least amount of time.

What should you do?

A. Run a platform security scanner on all instances in the organization.

B. Identify all external assets by using Cloud Asset Inventory, and then run a network security scanner against them.

C. Contact a Google approved security vendor to perform the audit.

D. Notify Google about the pending audit, and wait for confirmation before performing the scan.

Correct Answer: B

B. Identify all external assets by using Cloud Asset Inventory, and then run a network security scanner against them.

Cloud Asset Inventory allows you to see all of your Google Cloud assets. By using it, you can quickly identify which assets are externally accessible. Once identified, you can then run a specialized network security scanner against only these assets, making the process efficient. C. Contact a Google approved security vendor to perform the audit.

While using an external vendor can be beneficial for thoroughness, it may not meet the criteria of accomplishing the task in the "least amount of time."

QUESTION 3

A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer\\'s internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS

protection. They want to use GCP\\'s native SYN flood protection.

Which product should be used to meet these requirements?

A. Cloud Armor

B. VPC Firewall Rules

C. Cloud Identity and Access Management

D. Cloud CDN

Correct Answer: A

Reference: https://cloud.google.com/blog/products/identity-security/understanding-google-cloud-armors- new-waf-capabilities

QUESTION 4

You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually. You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket.

What should you do?

A. Set up an ACL with OWNER permission to a scope of allUsers.

B. Set up an ACL with READER permission to a scope of allUsers.

C. Set up a default bucket ACL and manage access for users using IAM.

D. Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

Correct Answer: D

https://cloud.google.com/storage/docs/uniform-bucket-level-access#enabled
https://cloud.google.com/storage/docs/access-control/lists

QUESTION 5

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

A. Central management of routes, firewalls, and VPNs for peered networks

B. Non-transitive peered networks; where only directly peered networks can communicate

C. Ability to peer networks that belong to different Google Cloud Platform organizations

D. Firewall rules that can be created with a tag from one peered network to another peered network

E. Ability to share specific subnets across peered networks

Correct Answer: BC

https://cloud.google.com/vpc/docs/vpc-peering#key_properties