# 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.leads4pass.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**

Which Google Cloud service should you use to enforce access control policies for applications and resources?

A. Identity-Aware Proxy

B. Cloud NAT

C. Google Cloud Armor

D. Shielded VMs

Correct Answer: A

https://cloud.google.com/iap/docs/concepts-overview "Use IAP when you want to enforce access control policies for applications and resources."

**QUESTION 2**

Your company\\'s Google Cloud organization has about 200 projects and 1,500 virtual machines. There is no uniform strategy for logs and events management, which reduces visibility for your security operations team. You need to design a logs management solution that provides visibility and allows the security team to view the environment\\'s configuration.

What should you do?

A. 1. Create a dedicated log sink for each project that is in scope.

2.

Use a BigQuery dataset with time partitioning enabled as a destination of the log sinks.

3.

Deploy alerts based on log metrics in every project.

4.

Grant the role "Monitoring Viewer" to the security operations team in each project.

B. 1. Create one log sink at the organization level that includes all the child resources.

2.

Use as destination a Pub/Sub topic to ingest the logs into the security information and event.

management (SIEM) on-premises, and ensure that the right team can access the SIEM.

3.

Grant the Viewer role at organization level to the security operations team.

C. 1. Enable network logs and data access logs for all resources in the "Production" folder.

2.

Do not create log sinks to avoid unnecessary costs and latency.

3.

Grant the roles "Logs Viewer" and "Browser" at project level to the security operations team.

D. 1. Create one sink for the "Production" folder that includes child resources and one sink for the logs ingested at the organization level that excludes child resources.

2.

As destination, use a log bucket with a minimum retention period of 90 days in a project that can be accessed by the security team.

3.

Grant the security operations team the role of Security Reviewer at organization level.

Correct Answer: B

B. 1. Create one log sink at the organization level that includes all the child resources.

2. Use as destination a Pub/Sub topic to ingest the logs into the security information and event management (SIEM) on-premises, and ensure that the right team can access the SIEM.

**QUESTION 3**

Your organization previously stored files in Cloud Storage by using Google Managed Encryption Keys (GMEK), but has recently updated the internal policy to require Customer Managed Encryption Keys (CMEK). You need to re-encrypt the files quickly and efficiently with minimal cost.

What should you do?

A. Reupload the files to the same Cloud Storage bucket specifying a key file by using gsutil.

B. Encrypt the files locally, and then use gsutil to upload the files to a new bucket.

C. Copy the files to a new bucket with CMEK enabled in a secondary region.

D. Change the encryption type on the bucket to CMEK, and rewrite the objects.

Correct Answer: D

https://cloud.google.com/storage/docs/encryption/using-customer-managed-keys

**QUESTION 4**

A company has redundant mail servers in different Google Cloud Platform regions and wants to route customers to the nearest mail server based on location. How should the company accomplish this?

A. Configure TCP Proxy Load Balancing as a global load balancing service listening on port 995.

B. Create a Network Load Balancer to listen on TCP port 995 with a forwarding rule to forward traffic based on location.

C. Use Cross-Region Load Balancing with an HTTP(S) load balancer to route traffic to the nearest region.

D. Use Cloud CDN to route the mail traffic to the closest origin mail server based on client IP address.

Correct Answer: A

https://cloud.google.com/load-balancing/docs/tcp https://cloud.google.com/load-balancing/docs/load-balancing-overview#tcp-proxy-load-balancing

TCP Proxy Load Balancing is implemented on GFEs that are distributed globally. If you choose the Premium Tier of Network Service Tiers, a TCP proxy load balancer is global. In Premium Tier, you can deploy backends in multiple regions, and the load balancer automatically directs user traffic to the closest region that has capacity. If you choose the Standard Tier, a TCP proxy load balancer can only direct traffic among backends in a single region.

**QUESTION 5**

You need to set up a Cloud interconnect connection between your company\\'s on-premises data center and VPC host network. You want to make sure that on-premises applications can only access Google APIs over the Cloud Interconnect and not through the public internet. You are required to only use APIs that are supported by VPC Service Controls to mitigate against exfiltration risk to non-supported APIs. How should you configure the network?

A. Enable Private Google Access on the regional subnets and global dynamic routing mode.

B. Set up a Private Service Connect endpoint IP address with the API bundle of "all-apis", which is advertised as a route over the Cloud interconnect connection.

C. Use private.googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the connection.

D. Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection.

Correct Answer: D

https://cloud.google.com/vpc/docs/private-service-connect

An API bundle: All APIs (all-apis): most Google APIs (same as private.googleapis.com). VPC-SC (vpc-sc): APIs that VPC Service Controls supports (same as restricted.googleapis.com). VMs in the same VPC network as the endpoint (all regions) On-premises systems that are connected to the VPC network that contains the endpoint