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.geekcert.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

You control network traffic for a folder in your Google Cloud environment. Your folder includes multiple projects and Virtual Private Cloud (VPC) networks. You want to enforce on the folder level that egress connections are limited only to IP range 10.58.5.0/24 and only from the VPC network "dev-vpc". You want to minimize implementation and maintenance effort.

What should you do?

A. 1. Leave the network configuration of the VMs in scope unchanged.

2.

Create a new project including a new VPC network "new-vpc".

3.

Deploy a network appliance in "new-vpc" to filter access requests and only allow egress connections from "dev-vpc" to 10.58.5.0/24.

B. 1. Leave the network configuration of the VMs in scope unchanged.

2. Enable Cloud NAT for "dev-vpc" and restrict the target range in Cloud NAT to 10.58.5.0/24.

C. 1. Attach external IP addresses to the VMs in scope.

2. Define and apply a hierarchical firewall policy on folder level to deny all egress connections and to allow egress to IP range 10.58.5.0/24 from network dev-vpc.

D. 1. Attach external IP addresses to the VMs in scope.

2. Configure a VPC Firewall rule in "dev-vpc" that allows egress connectivity to IP range 10.58.5.0/24 for all source addresses in this network.

Correct Answer: C

The correct answer is C. 1. Attach external IP addresses to the VMs in scope. 2. Define and apply a hierarchical firewall policy on folder level to deny all egress connections and to allow egress to IP range 10.58.5.0/24 from network dev-vpc.

This approach allows you to control network traffic at the folder level. By attaching external IP addresses to the VMs in scope, you can ensure that the VMs have a unique, routable IP address for outbound connections. Then, by defining and applying a hierarchical firewall policy at the folder level, you can enforce that egress connections are limited to the specified IP range and only from the specified VPC network.

QUESTION 2

Your Google Cloud organization allows for administrative capabilities to be distributed to each team through provision of a Google Cloud project with Owner role (roles/ owner). The organization contains thousands of Google Cloud Projects

Security Command Center Premium has surfaced multiple cpen_myscl_port findings. You are enforcing the guardrails and need to prevent these types of common misconfigurations.

What should you do?

A. Create a firewall rule for each virtual private cloud (VPC) to deny traffic from 0 0 0 0/0 with priority 0.

B. Create a hierarchical firewall policy configured at the organization to deny all connections from 0 0 0 0/0.

C. Create a Google Cloud Armor security policy to deny traffic from 0 0 0 0/0.

D. Create a hierarchical firewall policy configured at the organization to allow connections only from internal IP ranges

Correct Answer: B

QUESTION 3

Which Identity-Aware Proxy role should you grant to an Identity and Access Management (IAM) user to access HTTPS resources?

A. Security Reviewer

B. lAP-Secured Tunnel User

C. lAP-Secured Web App User

D. Service Broker Operator

Correct Answer: C

IAP-Secured Tunnel User: Grants access to tunnel resources that use IAP. IAP-Secured Web App User:

Access HTTPS resources which use Identity-Aware Proxy, Grants access to App Engine, Cloud Run, and Compute Engine resources. https://cloud.google.com/iap/docs/managing-access#roles

QUESTION 4

As adoption of the Cloud Data Loss Prevention (DLP) API grows within the company, you need to optimize usage to reduce cost. DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name.

Which cost reduction options should you recommend?

A. Set appropriate rowsLimit value on BigQuery data hosted outside the US and set appropriate bytesLimitPerFile value on multiregional Cloud Storage buckets.

B. Set appropriate rowsLimit value on BigQuery data hosted outside the US, and minimize transformation units on multiregional Cloud Storage buckets.

C. Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.

D. Use FindingLimits and TimespanContfig to sample data and minimize transformation units.

Correct Answer: C

https://cloud.google.com/dlp/docs/inspecting-storage#sampling https://cloud.google.com/dlp/docs/best-practices-costs#limit_scans_of_files_in_to_only_relevant_files Reference: https://cloud.google.com/dlp/docs/reference/rest/v2/InspectJobConfig

QUESTION 5

You plan to synchronize identities to Cloud Identity from a third-party identity provider (IdP). You discovered that some employees used their corporate email address to set up consumer accounts to access Google services. You need to

ensure that the organization has control over the configuration, security, and lifecycle of these consumer accounts.

What should you do? (Choose two.)

A. Mandate that those corporate employees delete their unmanaged consumer accounts.

B. Reconcile accounts that exist in Cloud Identity but not in the third-party IdP.

C. Evict the unmanaged consumer accounts in the third-party IdP before you sync identities.

D. Use Google Cloud Directory Sync (GCDS) to migrate the unmanaged consumer accounts\\' emails as user aliases.

E. Use the transfer tool to invite those corporate employees to transfer their unmanaged consumer accounts to the corporate domain.

Correct Answer: BE

To ensure control over the configuration, security, and lifecycle of consumer accounts created with corporate email addresses, you should reconcile accounts that exist in Cloud Identity but not in the third- party IdP (B). This helps to align accounts and ensure consistent management. Additionally, you can use the transfer tool to invite employees to transfer their unmanaged consumer accounts to the corporate domain (E), which allows you to bring these accounts under the organization\\'s control in Cloud Identity.