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.pass4itsure.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 is using GSuite and has developed an application meant for internal usage on Google App Engine. You need to make sure that an external user cannot gain access to the application even when an employee\\'s password has been compromised.

What should you do?

A. Enforce 2-factor authentication in GSuite for all users.

B. Configure Cloud Identity-Aware Proxy for the App Engine Application.

C. Provision user passwords using GSuite Password Sync.

D. Configure Cloud VPN between your private network and GCP.

Correct Answer: A

https://docs.google.com/document/d/11o3e14tyhnT7w45Q8-r9ZmTAfj2WUNUpJPZImrxm_F4/edit? usp=sharing
https://support.google.com/a/answer/175197?hl=en

QUESTION 2

You have an application where the frontend is deployed on a managed instance group in subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow thee application frontend to access the data in the application\\'s mysql instance on port 3306.

What should you do?

A. Configure an ingress firewall rule that allows communication from the src IP range of subnet A to the tag "data-tag" that is applied to the mysql Compute Engine VM on port 3306.

B. Configure an ingress firewall rule that allows communication from the frontend\\'s unique service account to the unique service account of the mysql Compute Engine VM on port 3306.

C. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an egress firewall rule that allows communication from Compute Engine VMs tagged with data-tag to destination Compute Engine VMs tagged fe-tag.

D. Configure a network tag "fe-tag" to be applied to all instances in subnet A and a network tag "data-tag" to be applied to all instances in subnet B. Then configure an ingress firewall rule that allows communication from Compute Engine VMs tagged with fe-tag to destination Compute Engine VMs tagged with data-tag.

Correct Answer: B

https://cloud.google.com/sql/docs/mysql/sql-proxy#using-a-service-account

QUESTION 3

Your team needs to make sure that a Compute Engine instance does not have access to the internet or to any Google

APIs or services. Which two settings must remain disabled to meet these requirements? (Choose two.)

A. Public IP

B. IP Forwarding

C. Private Google Access

D. Static routes

E. IAM Network User Role

Correct Answer: AC

Reference: https://cloud.google.com/vpc/docs/configure-private-google-access

QUESTION 4

Your team needs to prevent users from creating projects in the organization. Only the DevOps team should be allowed to create projects on behalf of the requester.

Which two tasks should your team perform to handle this request? (Choose two.)

A. Remove all users from the Project Creator role at the organizational level.

B. Create an Organization Policy constraint, and apply it at the organizational level.

C. Grant the Project Editor role at the organizational level to a designated group of users.

D. Add a designated group of users to the Project Creator role at the organizational level.

E. Grant the billing account creator role to the designated DevOps team.

Correct Answer: AD

https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints

QUESTION 5

You define central security controls in your Google Cloud environment for one of the folders in your organization you set an organizational policy to deny the assignment of external IP addresses to VMs. Two days later you receive an alert about a new VM with an external IP address under that folder.

What could have caused this alert?

A. The VM was created with a static external IP address that was reserved in the project before the organizational policy rule was set.

B. The organizational policy constraint wasn\\'t properly enforced and is running in "dry run mode.

C. At project level, the organizational policy control has been overwritten with an \\'allow\\' value.

D. The policy constraint on the folder level does not have any effect because of an allow" value for that constraint on the

organizational level.

Correct Answer: C