



# PROFESSIONAL-CLOUD-SECURITY-ENGINEER<sup>Q&As</sup>

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.passapply.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



VCE & PDF

PassApply.com

<https://www.passapply.com/professional-cloud-security-engineer.html>  
2024 Latest passapply PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF  
and VCE dumps Download

---

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

You have been tasked with implementing external web application protection against common web application attacks for a public application on Google Cloud. You want to validate these policy changes before they are enforced. What service should you use?

- A. Google Cloud Armor's preconfigured rules in preview mode
- B. Prepopulated VPC firewall rules in monitor mode
- C. The inherent protections of Google Front End (GFE)
- D. Cloud Load Balancing firewall rules
- E. VPC Service Controls in dry run mode

Correct Answer: A

Reference: <https://cloud.google.com/architecture/owasp-top-ten-mitigation> You can preview the effects of a rule without enforcing it. In preview mode, actions are noted in Cloud Monitoring. You can choose to preview individual rules in a security policy, or you can preview every rule in the policy. [https://cloud.google.com/armor/docs/security-policy-overview#preview\\_mode](https://cloud.google.com/armor/docs/security-policy-overview#preview_mode)

---

### QUESTION 2

The security operations team needs access to the security-related logs for all projects in their organization. They have the following requirements:

Follow the least privilege model by having only view access to logs.

Have access to Admin Activity logs.

Have access to Data Access logs.

Have access to Access Transparency logs.

Which Identity and Access Management (IAM) role should the security operations team be granted?

- A. roles/logging.privateLogViewer
- B. roles/logging.admin
- C. roles/viewer
- D. roles/logging.viewer

Correct Answer: A

<https://cloud.google.com/logging/docs/access-control#considerations> roles/logging.privateLogViewer (Private Logs Viewer) includes all the permissions contained by roles/logging.viewer, plus the ability to read Data Access audit logs in the \_Default bucket.

---



### QUESTION 3

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

Correct 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.

---

### QUESTION 4

You want to evaluate GCP for PCI compliance. You need to identify Google's inherent controls.

Which document should you review to find the information?

- A. Google Cloud Platform: Customer Responsibility Matrix
- B. PCI DSS Requirements and Security Assessment Procedures
- C. PCI SSC Cloud Computing Guidelines
- D. Product documentation for Compute Engine

Correct Answer: A

[https://cloud.google.com/files/PCI\\_DSS\\_Shared\\_Responsibility\\_GCP\\_v32.pdf](https://cloud.google.com/files/PCI_DSS_Shared_Responsibility_GCP_v32.pdf)  
[https://services.google.com/fh/files/misc/gcp\\_pci\\_shared\\_responsibility\\_matrix\\_aug\\_2021.pdf](https://services.google.com/fh/files/misc/gcp_pci_shared_responsibility_matrix_aug_2021.pdf)

---

### QUESTION 5

A customer's internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).

How should the team complete this task?

- A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.
- B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.



C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.

D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

Correct Answer: B

<https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#gsutil>

[Latest PROFESSIONAL-CLOUD-SECURITY-ENGINEER Dumps](#)

[PROFESSIONAL-CLOUD-SECURITY-ENGINEER PDF Dumps](#)

[PROFESSIONAL-CLOUD-SECURITY-ENGINEER Practice Test](#)