



# 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 need to connect your organization's on-premises network with an existing Google Cloud environment that includes one Shared VPC with two subnets named Production and Non-Production. You are required

to:

Use a private transport link.

Configure access to Google Cloud APIs through private API endpoints originating from on-premises environments.

Ensure that Google Cloud APIs are only consumed via VPC Service Controls.

What should you do?

- A. 1. Set up a Cloud VPN link between the on-premises environment and Google Cloud.  
2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.
- B. 1. Set up a Partner Interconnect link between the on-premises environment and Google Cloud.  
2. Configure private access using the private.googleapis.com domains in on-premises DNS configurations.
- C. 1. Set up a Direct Peering link between the on-premises environment and Google Cloud.  
2. Configure private access for both VPC subnets.
- D. 1. Set up a Dedicated Interconnect link between the on-premises environment and Google Cloud.  
2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.

Correct Answer: D

restricted.googleapis.com (199.36.153.4/30) only provides access to Cloud and Developer APIs that support VPC Service Controls. VPC Service Controls are enforced for these services <https://cloud.google.com/vpc/docs/configure-privategoogle-access-hybrid>

---

### QUESTION 2

A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack.

Which solution should this customer use?

- A. VPC Flow Logs
- B. Cloud Armor
- C. DNS Security Extensions
- D. Cloud Identity-Aware Proxy

Correct Answer: C



Reference: <https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns> DNSSEC --use a DNS registrar that supports DNSSEC, and enable it. DNSSEC digitally signs DNS communication, making it more difficult (but not impossible) for hackers to intercept and spoof. Domain Name System Security Extensions (DNSSEC) adds security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Having a trustworthy Domain Name System (DNS) that translates a domain name like [www.example.com](http://www.example.com) into its associated IP address is an increasingly important building block of today's web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites.  
<https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns>

---

### QUESTION 3

You manage a fleet of virtual machines (VMs) in your organization. You have encountered issues with lack of patching in many VMs. You need to automate regular patching in your VMs and view the patch management data across multiple projects.

What should you do? (Choose two.)

- A. View patch management data in VM Manager by using OS patch management.
- B. View patch management data in Artifact Registry.
- C. View patch management data in a Security Command Center dashboard.
- D. Deploy patches with Security Command Center by using Rapid Vulnerability Detection.
- E. Deploy patches with VM Manager by using OS patch management.

Correct Answer: AE

A. View patch management data in VM Manager by using OS patch management. VM Manager's OS patch management feature allows you to view patch compliance and deployment data across multiple projects.

E. Deploy patches with VM Manager by using OS patch management. VM Manager's OS patch management feature also allows you to automate the deployment of patches to your VMs.

---

### 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.p df](https://services.google.com/fh/files/misc/gcp_pci_shared_responsibility_matrix_aug_2021.pdf)

#### QUESTION 5

Which two implied firewall rules are defined on a VPC network? (Choose two.)

- A. A rule that allows all outbound connections
- B. A rule that denies all inbound connections
- C. A rule that blocks all inbound port 25 connections
- D. A rule that blocks all outbound connections
- E. A rule that allows all inbound port 80 connections

Correct Answer: AB

Implied IPv4 allow egress rule. An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination. Implied IPv4 deny ingress rule. An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them. [https://cloud.google.com/vpc/docs/firewalls?hl=en#default\\_firewall\\_rules](https://cloud.google.com/vpc/docs/firewalls?hl=en#default_firewall_rules)

#### QUESTION 6

You need to set up two network segments: one with an untrusted subnet and the other with a trusted subnet. You want to configure a virtual appliance such as a next-generation firewall (NGFW) to inspect all traffic between the two network segments.

How should you design the network to inspect the traffic?

- A. 1. Set up one VPC with two subnets: one trusted and the other untrusted.  
2. Configure a custom route for all traffic (0.0.0.0/0) pointed to the virtual appliance.
- B. 1. Set up one VPC with two subnets: one trusted and the other untrusted.  
2. Configure a custom route for all RFC1918 subnets pointed to the virtual appliance.
- C. 1. Set up two VPC networks: one trusted and the other untrusted, and peer them together.  
2. Configure a custom route on each network pointed to the virtual appliance.
- D. 1. Set up two VPC networks: one trusted and the other untrusted.  
2. Configure a virtual appliance using multiple network interfaces, with each interface connected to one of the VPC networks.

Correct Answer: D

Multiple network interfaces. The simplest way to connect multiple VPC networks through a virtual appliance is by using multiple network interfaces, with each interface connecting to one of the VPC networks. Internet and on-premises



connectivity is provided over one or two separate network interfaces. With many NGFW products, internet connectivity is connected through an interface marked as untrusted in the NGFW software.

<https://cloud.google.com/architecture/best-practices-vpc-design#l7>

This architecture has multiple VPC networks that are bridged by an L7 next-generation firewall (NGFW) appliance, which functions as a multi-NIC bridge between VPC networks. An untrusted, outside VPC network is introduced to terminate hybrid interconnects and internet-based connections that terminate on the outside leg of the L7 NGFW for inspection. There are many variations on this design, but the key principle is to filter traffic through the firewall before the traffic reaches trusted VPC networks.

## QUESTION 7

You need to implement an encryption-at-rest strategy that protects sensitive data and reduces key management complexity for non-sensitive data. Your solution has the following requirements:

1.

Schedule key rotation for sensitive data.

2.

Control which region the encryption keys for sensitive data are stored in.

3.

Minimize the latency to access encryption keys for both sensitive and non-sensitive data.

What should you do?

A. Encrypt non-sensitive data and sensitive data with Cloud External Key Manager.

B. Encrypt non-sensitive data and sensitive data with Cloud Key Management Service.

C. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud External Key Manager.

D. Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

Correct Answer: D

Google uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 Level 1 validated module, BoringCrypto, to implement encryption consistently across almost all Google Cloud products. To provide flexibility of controlling the key residency and rotation schedule, use google provided key for non-sensitive and encrypt sensitive data with Cloud Key Management Service

## QUESTION 8

In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized. Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

A. App Engine



- B. Cloud Functions
- C. Compute Engine
- D. Google Kubernetes Engine
- E. Cloud Storage

Correct Answer: CD

App Engine ingress firewall rules are available, but egress rules are not currently available. Per requirements 1.2.1 and 1.3.4, you must ensure that all outbound traffic is authorized. SAQ A-EP and SAQ D-Type merchants must provide compensating controls or use a different Google Cloud product. Compute Engine and GKE are the preferred alternatives. <https://cloud.google.com/solutions/pci-dss-compliance-in-gcp>

---

#### QUESTION 9

You have been tasked with inspecting IP packet data for invalid or malicious content. What should you do?

- A. Use Packet Mirroring to mirror traffic to and from particular VM instances. Perform inspection using security software that analyzes the mirrored traffic.
- B. Enable VPC Flow Logs for all subnets in the VPC. Perform inspection on the Flow Logs data using Cloud Logging.
- C. Configure the Fluentd agent on each VM Instance within the VPC. Perform inspection on the log data using Cloud Logging.
- D. Configure Google Cloud Armor access logs to perform inspection on the log data.

Correct Answer: A

<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 10

You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.

What should you do?

- A. Migrate the application into an isolated project using a "Lift and Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
- B. Migrate the application into an isolated project using a "Lift and Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
- C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.



D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

Correct Answer: A

Migrate the application into an isolated project using a "Lift and Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

---

### QUESTION 11

You are deploying a web application hosted on Compute Engine. A business requirement mandates that application logs are preserved for 12 years and data is kept within European boundaries. You want to implement a storage solution that minimizes overhead and is cost-effective. What should you do?

- A. Create a Cloud Storage bucket to store your logs in the EUROPE-WEST1 region. Modify your application code to ship logs directly to your bucket for increased efficiency.
- B. Configure your Compute Engine instances to use the Google Cloud's operations suite Cloud Logging agent to send application logs to a custom log bucket in the EUROPE-WEST1 region with a custom retention of 12 years.
- C. Use a Pub/Sub topic to forward your application logs to a Cloud Storage bucket in the EUROPE- WEST1 region.
- D. Configure a custom retention policy of 12 years on your Google Cloud's operations suite log bucket in the EUROPE-WEST1 region.

Correct Answer: B

<https://youtu.be/MI4iG2GIZMA>

---

### QUESTION 12

You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys.

What should you do?

- A. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the Key level.
- B. Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.
- C. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the Key level.
- D. Create a KeyRing per persistent disk, with each KeyRing containing a single Key. Manage the IAM permissions at the KeyRing level.

Correct Answer: B

<https://cloud.netapp.com/blog/gcp-cvo-blg-how-to-use-google-cloud-encryption-with-a-persistent-disk>

---





### QUESTION 13

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 14

You're developing the incident response plan for your company. You need to define the access strategy that your DevOps team will use when reviewing and investigating a deployment issue in your Google Cloud environment. There are two

main requirements:

Least-privilege access must be enforced at all times. The DevOps team must be able to access the required resources only during the deployment issue.

How should you grant access while following Google-recommended best practices?

- A. Assign the Project Viewer Identity and Access Management (IAM) role to the DevOps team.
- B. Create a custom IAM role with limited list/view permissions, and assign it to the DevOps team.
- C. Create a service account, and grant it the Project Owner IAM role. Give the Service Account User Role on this service account to the DevOps team.
- D. Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team.

Correct Answer: B

---

### QUESTION 15

You want to use the gcloud command-line tool to authenticate using a third-party single sign-on (SSO) SAML identity provider. Which options are necessary to ensure that authentication is supported by the third-party identity provider (IdP)? (Choose two.)

- A. SSO SAML as a third-party IdP
- B. Identity Platform



- C. OpenID Connect
- D. Identity-Aware Proxy
- E. Cloud Identity

Correct Answer: AC

To provide users with SSO-based access to selected cloud apps, Cloud Identity as your IdP supports the OpenID Connect (OIDC) and Security Assertion Markup Language 2.0 (SAML) protocols. <https://cloud.google.com/identity/solutions/enable-ssso>

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

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

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