

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

Professional Cloud Network Engineer

**Pass Google PROFESSIONAL-CLOUD-NETWORK-  
ENGINEER Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/professional-cloud-network-engineer.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by Google  
Official Exam Center

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



### QUESTION 1

You need to restrict access to your Google Cloud load-balanced application so that only specific IP addresses can connect.

What should you do?

- A. Create a secure perimeter using the Access Context Manager feature of VPC Service Controls and restrict access to the source IP range of the allowed clients and Google health check IP ranges.
- B. Create a secure perimeter using VPC Service Controls, and mark the load balancer as a service restricted to the source IP range of the allowed clients and Google health check IP ranges.
- C. Tag the backend instances "application," and create a firewall rule with target tag "application" and the source IP range of the allowed clients and Google health check IP ranges.
- D. Label the backend instances "application," and create a firewall rule with the target label "application" and the source IP range of the allowed clients and Google health check IP ranges.

Correct Answer: C

Reference: [https://link.springer.com/chapter/10.1007/978-1-4842-1004-8\\_4](https://link.springer.com/chapter/10.1007/978-1-4842-1004-8_4)

---

### QUESTION 2

Your company offers a popular gaming service. Your instances are deployed with private IP addresses, and external access is granted through a global load balancer. You believe you have identified a potential malicious actor, but aren't certain you have the correct client IP address. You want to identify this actor while minimizing disruption to your legitimate users.

What should you do?

- A. Create a Cloud Armor Policy rule that denies traffic and review necessary logs.
- B. Create a Cloud Armor Policy rule that denies traffic, enable preview mode, and review necessary logs.
- C. Create a VPC Firewall rule that denies traffic, enable logging and set enforcement to disabled, and review necessary logs.
- D. Create a VPC Firewall rule that denies traffic, enable logging and set enforcement to enabled, and review necessary logs.

Correct Answer: D

---

### QUESTION 3

You need to create a new VPC network that allows instances to have IP addresses in both the 10.1.1.0/24 network and the 172.16.45.0/24 network.

What should you do?

- A. Configure global load balancing to point 172.16.45.0/24 to the correct instance.
- B. Create unique DNS records for each service that sends traffic to the desired IP address.
- C. Configure an alias-IP range of 172.16.45.0/24 on the virtual instances within the VPC subnet of 10.1.1.0/24.
- D. Use VPC peering to allow traffic to route between the 10.1.0.0/24 network and the 172.16.45.0/24 network.

Correct Answer: B

---

#### QUESTION 4

You are configuring a new instance of Cloud Router in your Organization's Google Cloud environment to allow connection across a new Dedicated Interconnect to your data center. Sales, Marketing, and IT each have a service project attached to the Organization's host project.

Where should you create the Cloud Router instance?

- A. VPC network in all projects
- B. VPC network in the IT Project
- C. VPC network in the Host Project
- D. VPC network in the Sales, Marketing, and IT Projects

Correct Answer: C

Reference: <https://cloud.google.com/interconnect/docs/how-to/dedicated/using-interconnects-otherprojects>

---

#### QUESTION 5

You decide to set up Cloud NAT. After completing the configuration, you find that one of your instances is not using the Cloud NAT for outbound NAT.

What is the most likely cause of this problem?

- A. The instance has been configured with multiple interfaces.
- B. An external IP address has been configured on the instance.
- C. You have created static routes that use RFC1918 ranges.
- D. The instance is accessible by a load balancer external IP address.

Correct Answer: B

Reference: <https://www.sovereignsolutionscorp.com/google-cloud-nat/>

---

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

[PROFESSIONAL-CLOUD-NETWORK-ENGINEER Study Guide](#)

[PROFESSIONAL-CLOUD-NETWORK-ENGINEER Braindumps](#)