

PROFESSIONAL-CLOUD-NETWORK-ENGINEER^{Q&As}

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.leads4pass.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

Your software team is developing an on-premises web application that requires direct connectivity to Compute Engine Instances in GCP using the RFC 1918 address space. You want to choose a connectivity solution from your on-premises environment to GCP, given these specifications:

1.

Your ISP is a Google Partner Interconnect provider.

2.

Your on-premises VPN device's internet uplink and downlink speeds are 10 Gbps.

3.

A test VPN connection between your on-premises gateway and GCP is performing at a maximum speed of 500 Mbps due to packet losses.

4.

Most of the data transfer will be from GCP to the on-premises environment.

5.

The application can burst up to 1.5 Gbps during peak transfers over the Interconnect.

6.

Cost and the complexity of the solution should be minimal.

How should you provision the connectivity solution?

A. Provision a Partner Interconnect through your ISP.

B. Provision a Dedicated Interconnect instead of a VPN.

C. Create multiple VPN tunnels to account for the packet losses, and increase bandwidth using ECMP.

D. Use network compression over your VPN to increase the amount of data you can send over your VPN.

Correct Answer: C

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 want to deploy a VPN Gateway to connect your on-premises network to GCP. You are using a non BGP-capable on-premises VPN device. You want to minimize downtime and operational overhead when your network grows. The device supports only IKEv2, and you want to follow Google-recommended practices.

What should you do?

- A. Create a Cloud VPN instance. Create a policy-based VPN tunnel per subnet. Configure the appropriate local and remote traffic selectors to match your local and remote networks. Create the appropriate static routes.
- B. Create a Cloud VPN instance. Create a policy-based VPN tunnel. Configure the appropriate local and remote traffic selectors to match your local and remote networks. Configure the appropriate static routes.
- C. Create a Cloud VPN instance. Create a route-based VPN tunnel. Configure the appropriate local and remote traffic selectors to match your local and remote networks. Configure the appropriate static routes.
- D. Create a Cloud VPN instance. Create a route-based VPN tunnel. Configure the appropriate local and remote traffic selectors to 0.0.0.0/0. Configure the appropriate static routes.

Correct Answer: D

Reference: <https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing>

QUESTION 4

You have an application hosted on a Compute Engine virtual machine instance that cannot communicate with a resource outside of its subnet. When you review the flow and firewall logs, you do not see any denied traffic listed.

During troubleshooting you find:

1.

Flow logs are enabled for the VPC subnet, and all firewall rules are set to log.

2.

The subnetwork logs are not excluded from Stackdriver.

3.

The instance that is hosting the application can communicate outside the subnet.

4.

Other instances within the subnet can communicate outside the subnet.

5.

The external resource initiates communication.

What is the most likely cause of the missing log lines?

- A. The traffic is matching the expected ingress rule.
- B. The traffic is matching the expected egress rule.
- C. The traffic is not matching the expected ingress rule.
- D. The traffic is not matching the expected egress rule.

Correct Answer: C

QUESTION 5

You need to define an address plan for a future new GKE cluster in your VPC. This will be a VPC-native cluster, and the default Pod IP range allocation will be used. You must pre-provision all the needed VPC subnets and their respective IP address ranges before cluster creation. The cluster will initially have a single node, but it will be scaled to a maximum of three nodes if necessary. You want to allocate the minimum number of Pod IP addresses.

Which subnet mask should you use for the Pod IP address range?

- A. /21
- B. /22
- C. /23
- D. /25

Correct Answer: D

Reference: <https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips>

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

[PROFESSIONAL-CLOUD-NETWORK-ENGINEER Exam Questions](#)

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