



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.geekcert.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



VCE & PDF

GeekCert.com

<https://www.geekcert.com/professional-cloud-network-engineer.html>
2024 Latest geekcert PROFESSIONAL-CLOUD-NETWORK-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 are responsible for designing a new connectivity solution between your organization's on-premises data center and your Google Cloud Virtual Private Cloud (VPC) network. Currently, there is no end-to-end connectivity. You must ensure a service level agreement (SLA) of 99.99% availability. What should you do?

- A. Use one Dedicated Interconnect connection in a single metropolitan area. Configure one Cloud Router and enable global routing in the VPC.
- B. Use a Direct Peering connection between your on-premises data center and Google Cloud. Configure Classic VPN with two tunnels and one Cloud Router.
- C. Use two Dedicated Interconnect connections in a single metropolitan area. Configure one Cloud Router and enable global routing in the VPC.
- D. Use HA VPN. Configure one tunnel from each interface of the VPN gateway to connect to the corresponding interfaces on the peer gateway on-premises. Configure one Cloud Router and enable global routing in the VPC.

Correct Answer: B

QUESTION 2

Your company has provisioned 2000 virtual machines (VMs) in the private subnet of your Virtual Private Cloud (VPC) in the us-east1 region. You need to configure each VM to have a minimum of 128 TCP connections to a public repository so that users can download software updates and packages over the internet. You need to implement a Cloud NAT gateway so that the VMs are able to perform outbound NAT to the internet. You must ensure that all VMs can simultaneously connect to the public repository and download software updates and packages. Which two methods can you use to accomplish this? (Choose two.)

- A. Configure the NAT gateway in manual allocation mode, allocate 2 NAT IP addresses, and update the minimum number of ports per VM to 256.
- B. Create a second Cloud NAT gateway with the default minimum number of ports configured per VM to 64.
- C. Use the default Cloud NAT gateway's NAT proxy to dynamically scale using a single NAT IP address.
- D. Use the default Cloud NAT gateway to automatically scale to the required number of NAT IP addresses, and update the minimum number of ports per VM to 128.
- E. Configure the NAT gateway in manual allocation mode, allocate 4 NAT IP addresses, and update the minimum number of ports per VM to 128.

Correct Answer: AB

QUESTION 3

Your company's security team wants to limit the type of inbound traffic that can reach your web servers to protect against security threats. You need to configure the firewall rules on the web servers within your Virtual Private Cloud (VPC) to handle HTTP and HTTPS web traffic for TCP only. What should you do?

- A. Create an allow on match ingress firewall rule with the target tag "web-server" to allow all IP addresses for TCP port



80.

B. Create an allow on match egress firewall rule with the target tag "web-server" to allow all IP addresses for TCP port 80.

C. Create an allow on match ingress firewall rule with the target tag "web-server" to allow all IP addresses for TCP ports 80 and 443.

D. Create an allow on match egress firewall rule with the target tag "web-server" to allow web server IP addresses for TCP ports 60 and 443.

Correct Answer: C

Reference: <https://cloud.google.com/load-balancing/docs/https>

QUESTION 4

Your company has recently installed a Cloud VPN tunnel between your on-premises data center and your Google Cloud Virtual Private Cloud (VPC). You need to configure access to the Cloud Functions API for your on-premises servers. The configuration must meet the following requirements:

Certain data must stay in the project where it is stored and not be exfiltrated to other projects.

Traffic from servers in your data center with RFC 1918 addresses do not use the internet to access Google Cloud APIs.

All DNS resolution must be done on-premises.

The solution should only provide access to APIs that are compatible with VPC Service Controls.

What should you do?

A. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range. Create a CNAME record for *.googleapis.com that points to the A record. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record. Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.

B. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range. Create a CNAME record for *.googleapis.com that points to the A record. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record. Configure your on-premises firewalls to allow traffic to the restricted.googleapis.com addresses.

C. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range. Create a CNAME record for *.googleapis.com that points to the A record. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record. Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.

D. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range. Create a CNAME record for *.googleapis.com that points to the A record. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record. Configure your on-premises firewalls to allow traffic to the private.googleapis.com addresses.

Correct Answer: C

**QUESTION 5**

You are configuring load balancing for a standard three-tier (web, application, and database) application. You have configured an external HTTP(S) load balancer for the web servers. You need to configure load balancing for the application tier of servers. What should you do?

- A. Configure a forwarding rule on the existing load balancer for the application tier.
- B. Configure equal cost multi-path routing on the application servers.
- C. Configure a new internal HTTP(S) load balancer for the application tier.
- D. Configure a URL map on the existing load balancer to route traffic to the application tier.

Correct Answer: A

[Latest PROFESSIONAL-CL
OUD-NETWORK-
ENGINEER Dumps](#)

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

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