Free Questions for Professional-Cloud-Network-Engineer by vceexamstest

Shared by Kelley on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

You are designing a hub-and-spoke network architecture for your company's cloud-based environment. You need to make sure that all spokes are peered with the hub. The spokes must use the hub's virtual appliance for internet access.

The virtual appliance is configured in high-availability mode with two instances using an internal load balancer with IP address 10.0.0.5. What should you do?

Options:

A- Create a default route in the hub VPC that points to IP address 10.0.0.5.
Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway.
Export the custom routes in the hub.
Import the custom routes in the spokes.

B- Create a default route in the hub VPC that points to IP address 10.0.0.5.
Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway.
Export the custom routes in the hub. Import the custom routes in the spokes.
Delete the default internet gateway route of the spokes.

C- Create two default routes in the hub VPC that point to the next hop instances of the virtual appliances.

Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway.

Export the custom routes in the hub. Import the custom routes in the spokes.

D- Create a default route in the hub VPC that points to IP address 10.0.0.5.

Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway.

Create a new route in the spoke VPC that points to IP address 10.0.0.5.

Answer:

B

Question 2

You are responsible for enabling Private Google Access for the virtual machine (VM) instances in your Virtual Private Cloud (VPC) to access Google APIs. All VM instances have only a private IP address and need to access Cloud Storage. You need to ensure that all VM traffic is routed back to your on-premises data center for traffic scrubbing via your existing Cloud Interconnect connection. However, VM traffic to Google APIs should remain in the VPC. What should you do?

Options:

A- Delete the default route in your VPC.

Create a private Cloud DNS zone for googleapis.com, create a CNAME for *.googleapis.com to restricted googleapis.com, and create an A record for restricted googleapis com that resolves to the addresses in 199.36.153.4/30.

Create a static route in your VPC for the range 199.36.153.4/30 with the default internet gateway as the next hop.

B- Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP).

Create a public Cloud DNS zone with a CNAME for *.google.com to private googleapis com, create a CNAME for * googleapis.com to private googleapis com, and create an A record for Private googleapis.com that resolves to the addresses in 199.36.153 8/30.

Create a static route in your VPC for the range 199 .36.153.8/30 with the default internet gateway as the next hop.

C- Configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP) with a lower priority (MED) than the default VPC route.

Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googieapis.com to private googleapis com, and create an A record for private.googleapis.com that resolves to the addresses in 199 .36.153.8/30.

Create a static route in your VPC for the range 199.36. 153.8/30 with the default internet gateway as the next hop.

D- Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP).

Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googieapis.com to Private googleapis.com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30.

Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.

Answer:

C

Question 3

You recently deployed two network virtual appliances in us-central1. Your network appliances provide connectivity to your on-premises network, 10.0.0.0/8. You need to configure the routing for your Virtual Private Cloud (VPC). Your design must meet the following requirements:

All access to your on-premises network must go through the network virtual appliances.

Allow on-premises access in the event of a single network virtual appliance failure.

Both network virtual appliances must be used simultaneously.

Which method should you use to accomplish this?

Options:

A- Configure two routes for 10.0.0.0/8 with different priorities, each pointing to separate network virtual appliances.

B- Configure an internal HTTP(S) load balancer with the two network virtual appliances as backends. Configure a route for 10.0.0.0/8 with the internal HTTP(S) load balancer as the next hop.

C- Configure a network load balancer for the two network virtual appliances. Configure a route for 10.0.0.0/8 with the network load balancer as the next hop.

D- Configure an internal TCP/UDP load balancer with the two network virtual appliances as backends. Configure a route for 10.0.0.0/8

with the internal load balancer as the next hop.

Answer:

B

Question 4

Question Type: **MultipleChoice**

You have an HA VPN connection with two tunnels running in active/passive mode between your Virtual Private Cloud (VPC) and on-premises network. Traffic over the connection has recently increased from 1 gigabit per second (Gbps) to 4 Gbps, and you notice that packets are being dropped. You need to configure your VPN connection to Google Cloud to support 4 Gbps. What should you do?

Options:

A- Configure the remote autonomous system number (ASN) to 4096.

B- Configure a second Cloud Router to scale bandwidth in and out of the VPC.

C- Configure the maximum transmission unit (MTU) to its highest supported value.

D- Configure a second set of active/passive VPN tunnels.

Answer:

D

Question 5

Question Type: MultipleChoice

You built a web application with several containerized microservices. You want to run those microservices on Cloud Run. You must also ensure that the services are highly available to your customers with low latency. What should you do?

Options:

A- Deploy the Cloud Run services to multiple availability zones. Create a global TCP load balancer. Add the Cloud Run endpoints to its backend service.

B- Deploy the Cloud Run services to multiple regions. Create serverless network endpoint groups (NEGs) that point to the services. Create a global HTTPS load balancer, and attach the serverless NEGs as backend services of the load balancer.

C- Deploy the Cloud Run services to multiple availability zones. Create Cloud Endpoints that point to the services. Create a global HTTPS load balancer, and attach the Cloud Endpoints to its backend

D- Deploy the Cloud Run services to multiple regions. Configure a round-robin A record in Cloud DNS.

Answer:

B

Question 6

Question Type: MultipleChoice

Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with on-premises connectivity already in place. You are deploying a new application using Google Kubernetes Engine (GKE), which must be accessible only from the same VPC network and on-premises locations. You must ensure that the GKE control plane is exposed to a predefined list of on-premises subnets through private connectivity only. What should you do?

Options:

A- Create a GKE private cluster with a private endpoint for the control plane. Configure VPC Networking Peering export/import routes and custom route advertisements on the Cloud Routers. Configure authorized networks to specify the desired on-premises subnets.

B- Create a GKE private cluster with a public endpoint for the control plane. Configure VPC Networking Peering export/import routes and custom route advertisements on the Cloud Routers.

C- Create a GKE private cluster with a private endpoint for the control plane. Configure authorized networks to specify the desired on-premises subnets.

D- Create a GKE public cluster. Configure authorized networks to specify the desired on-premises subnets.

Answer:

C

Question 7

Question Type: **MultipleChoice**

You are designing a hybrid cloud environment for your organization. Your Google Cloud environment is interconnected with your on-premises network using Cloud HA VPN and Cloud Router. The Cloud Router is configured with the default settings. Your on-premises DNS server is located at 192.168.20.88 and is protected by a firewall, and your Compute Engine resources are located at 10.204.0.0/24. Your Compute Engine resources need to resolve on-premises private hostnames using the domain corp.altostrat.com while still resolving Google Cloud hostnames. You want to follow Google-recommended practices. What should you do?

Options:

A- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
Configure your on-premises firewall to accept traffic from 10.204.0.0/24.
Set a custom route advertisement on the Cloud Router for 10.204.0.0/24

B- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168 20.88.

Configure your on-premises firewall to accept traffic from 35.199.192.0/19

Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.

C- Create a private forwarding zone in Cloud DNS for 'corp .altostrat.com' called corp-altostrat-com that points to 192.168.20.88.

Configure your on-premises firewall to accept traffic from 10.204.0.0/24.

Modify the /etc/resolv conf file on your Compute Engine instances to point to 192.168.20 88

D- Create a private zone in Cloud DNS for 'corp altostrat.com' called corp-altostrat-com.

Configure DNS Server Policies and create a policy with Alternate DNS servers to 192.168.20.88.

Configure your on-premises firewall to accept traffic from 35.199.192.0/19.

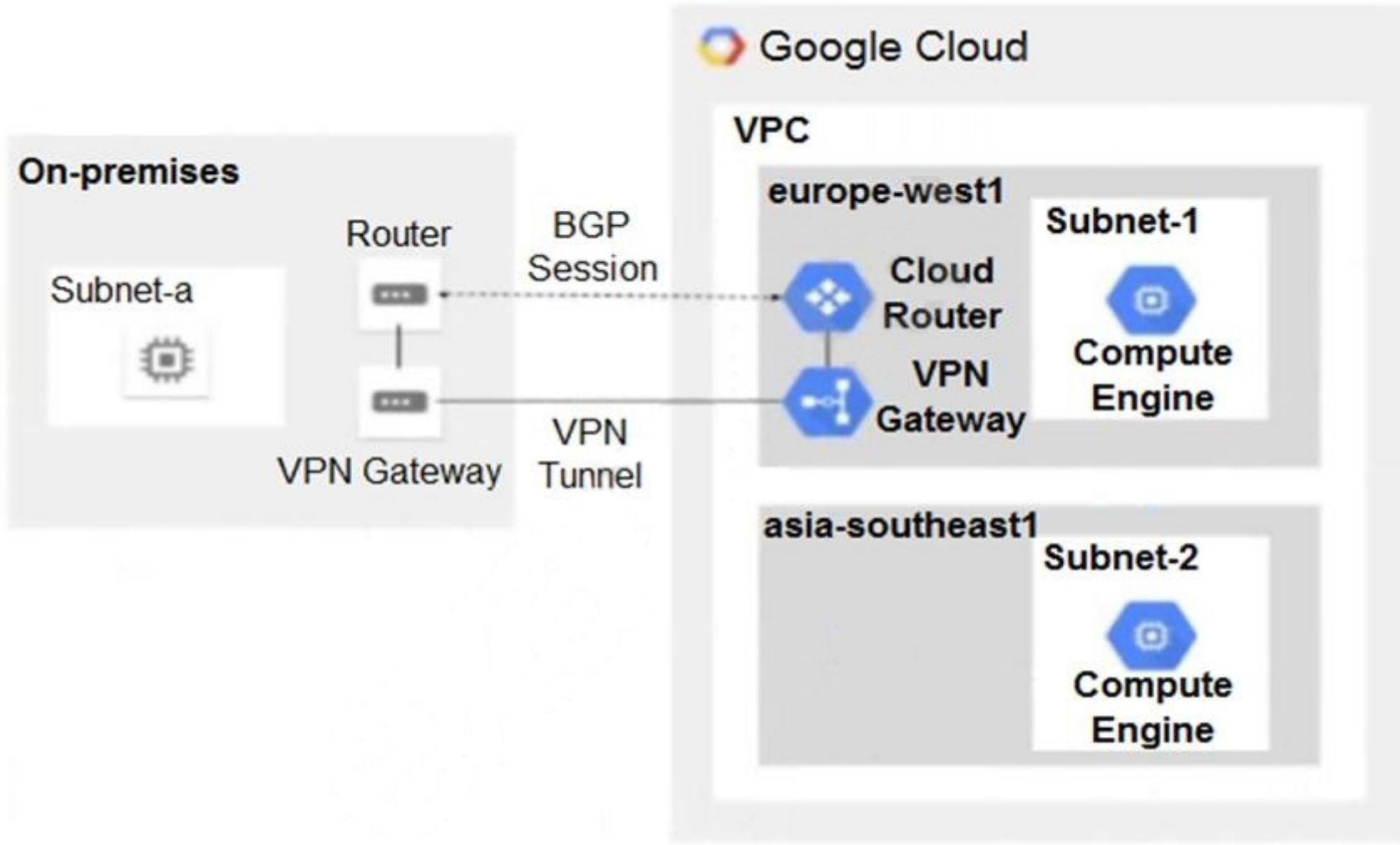Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.

Answer:

D

Question 8

Question Type: MultipleChoice

You have the following routing design. You discover that Compute Engine instances in Subnet-2 in the asia-southeast1 region cannot communicate with compute resources on-premises. What should you do?

On-premises

Subnet-a

Router

BGP Session

VPN Gateway

VPN Tunnel

Google Cloud

VPC

europe-west1

Cloud Router

VPN Gateway

Subnet-1

Compute Engine

asia-southeast1

Subnet-2

Compute Engine

Options:

A- Configure a custom route advertisement on the Cloud Router.

B- Enable IP forwarding in the asia-southeast1 region.

C- Change the VPC dynamic routing mode to Global.

D- Add a second Border Gateway Protocol (BGP) session to the Cloud Router.

Answer:

C