# Google

## Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer

**NEW QUESTION 1**
You are configuring a new application that will be exposed behind an external load balancer with both IPv4 and IPv6 addresses and support TCP pass-through on port 443. You will have backends in two regions:
us-west1 and us-east1. You want to serve the content with the lowest possible latency while ensuring high availability and autoscaling. Which configuration should you use?

A. Use global SSL Proxy Load Balancing with backends in both regions.
B. Use global TCP Proxy Load Balancing with backends in both regions.
C. Use global external HTTP(S) Load Balancing with backends in both regions.
D. Use Network Load Balancing in both regions, and use DNS-based load balancing to direct traffic to the closest region.

**Answer:** D

**NEW QUESTION 2**
You have a Cloud Storage bucket in Google Cloud project XYZ. The bucket contains sensitive data. You need to design a solution to ensure that only instances belonging to VPCs under project XYZ can access the data stored in this Cloud Storage bucket. What should you do?

A. Configure Private Google Access to privately access the Cloud Storage service using private IP addresses.
B. Configure a VPC Service Controls perimeter around project XYZ, and include storage.googleapis.com as a restricted service in the service perimeter.
C. Configure Cloud Storage with projectPrivate Access Control List (ACL) that gives permission to the project team based on their roles.
D. Configure Private Service Connect to privately access Cloud Storage from all VPCs under project XYZ.

**Answer:** C

**NEW QUESTION 3**
You have an application that is running in a managed instance group. Your development team has released an updated instance template which contains a new feature which was not heavily tested. You want to minimize impact to users if there is a bug in the new template.
How should you update your instances?

A. Manually patch some of the instances, and then perform a rolling restart on the instance group.
B. Using the new instance template, perform a rolling update across all instances in the instance group.Verify the new feature once the rollout completes.
C. Deploy a new instance group and canary the updated template in that grou
D. Verify the new feature in the new canary instance group, and then update the original instance group.
E. Perform a canary update by starting a rolling update and specifying a target size for your instances to receive the new templat
F. Verify the new feature on the canary instances, and then roll forward to the rest of the instances.

**Answer:** D

**Explanation:**
https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups#startin https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups

**NEW QUESTION 4**
You need to define an address plan for a future new Google Kubernetes Engine (GKE) cluster in your Virtual Private Cloud (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

**Answer:** A

**NEW QUESTION 5**
You have just deployed your infrastructure on Google Cloud. You now need to configure the DNS to meet the following requirements:
Your on-premises resources should resolve your Google Cloud zones. Your Google Cloud resources should resolve your on-premises zones.
You need the ability to resolve ".internal" zones provisioned by Google Cloud. What should you do?

A. Configure an outbound server policy, and set your alternative name server to be your on-premises DNS resolve
B. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google's public DNS 8.8.8.8.
C. Configure both an inbound server policy and outbound DNS forwarding zones with the target as the on-premises DNS resolve
D. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google Cloud's DNS resolver.
E. Configure an outbound DNS server policy, and set your alternative name server to be your on-premises DNS resolve
F. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google Cloud's DNS resolver.
G. Configure Cloud DNS to DNS peer with your on-premises DNS resolve
H. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google's public DNS 8.8.8.8.

**Answer:** A

**NEW QUESTION 6**
You converted an auto mode VPC network to custom mode. Since the conversion, some of your Cloud Deployment Manager templates are no longer working.
You want to resolve the problem.
What should you do?

A. Apply an additional IAM role to the Google API's service account to allow custom mode networks.
B. Update the VPC firewall to allow the Cloud Deployment Manager to access the custom mode networks.
C. Explicitly reference the custom mode networks in the Cloud Armor whitelist.
D. Explicitly reference the custom mode networks in the Deployment Manager templates.

**Answer:** D

**NEW QUESTION 7**
You need to enable Cloud CDN for all the objects inside a storage bucket. You want to ensure that all the object in the storage bucket can be served by the CDN. What should you do in the GCP Console?

A. Create a new cloud storage bucket, and then enable Cloud CDN on it.
B. Create a new TCP load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.
C. Create a new SSL proxy load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.
D. Create a new HTTP load balancer, select the storage bucket as a backend, enable Cloud CDN on the backend, and make sure each object inside the storage bucket is shared publicly.

**Answer:** D

**Explanation:**
https://cloud.google.com/load-balancing/docs/https/adding-backend-buckets-to-load-balancers#using_cloud_cdn Cloud CDN needs HTTP(S) Load Balancers and Cloud Storage bucket has to be shared publicly.
https://cloud.google.com/cdn/docs/setting-up-cdn-with-bucket

**NEW QUESTION 8**
You created a new VPC network named Dev with a single subnet. You added a firewall rule for the network Dev to allow HTTP traffic only and enabled logging. When you try to log in to an instance in the subnet via Remote Desktop Protocol, the login fails. You look for the Firewall rules logs in Stackdriver Logging, but you do not see any entries for blocked traffic. You want to see the logs for blocked traffic.
What should you do?

A. Check the VPC flow logs for the instance.
B. Try connecting to the instance via SSH, and check the logs.
C. Create a new firewall rule to allow traffic from port 22, and enable logs.
D. Create a new firewall rule with priority 65500 to deny all traffic, and enable logs.

**Answer:** D

**Explanation:**
Ingress packets in VPC Flow Logs are sampled after ingress firewall rules. If an ingress firewall rule denies inbound packets, those packets are not sampled by VPC Flow Logs. We want to see the logs for blocked traffic so we have to look for them in firewall logs.
https://cloud.google.com/vpc/docs/flow-logs#key_properties

**NEW QUESTION 9**
You need to enable Private Google Access for use by some subnets within your Virtual Private Cloud (VPC). Your security team set up the VPC to send all internet-bound traffic back to the on- premises data center for inspection before egressing to the internet, and is also implementing VPC Service Controls in the environment for API-level security control. You have already enabled the subnets for Private Google Access. What configuration changes should you make to enable Private Google Access while adhering to your security team's requirements?

A. Create a private DNS zone with a CNAME record for *.googleapis.com to restricted.googleapis.com, with an A record pointing to Google's restricted API address range.Create a custom route that points Google's restricted API address range to the default internet gateway as the next hop.
B. Create a private DNS zone with a CNAME record for *.googleapis.com to restricted.googleapis.com, with an A record pointing to Google's restricted API address range.Change the custom route that points the default route (0/0) to the default internet gateway as the next hop.
C. Create a private DNS zone with a CNAME record for *.googleapis.com to private.googleapis.com, with an A record painting to Google's private AP address range.Change the custom route that points the default route (0/0) to the default internet gateway as the next hop.
D. Create a private DNS zone with a CNAME record for *.googleapis.com to private.googleapis.com, with an A record pointing to Google's private API address range.Create a custom route that points Google's private API address range to the default internet gateway as the next hop.

**Answer:** C

**NEW QUESTION 10**
You need to configure a Google Kubernetes Engine (GKE) cluster. The initial deployment should have 5 nodes with the potential to scale to 10 nodes. The maximum number of Pods per node is 8. The number of services could grow from 100 to up to 1024. How should you design the IP schema to optimally meet this requirement?

A. Configure a /28 primary IP address range for the node IP addresse
B. Configure a (25 secondary IP range for the Pod
C. Configure a /22 secondary IP range for the Services.
D. Configure a /28 primary IP address range for the node IP addresse
E. Configure a /25 secondary IP range for the Pod
F. Configure a /21 secondary IP range for the Services.
G. Configure a /28 primary IP address range for the node IP addresse
H. Configure a /28 secondary IP range for the Pod
I. Configure a /21 secondary IP range for the Services.
J. Configure a /28 primary IP address range for the node IP addresse
K. Configure a /24 secondary IP range for the Pad
L. Configure a /22 secondary IP range for the Services.

**Answer:** A

**NEW QUESTION 10**
You want to establish a dedicated connection to Google that can access Cloud SQL via a public IP address and that does not require a third-party service provider.
Which connection type should you choose?

A. Carrier Peering
B. Direct Peering
C. Dedicated Interconnect
D. Partner Interconnect

**Answer:** B

**Explanation:**
When established, Direct Peering provides a direct path from your on-premises network to Google services, including Google Cloud products that can be exposed through one or more public IP addresses. Traffic from Google's network to your on-premises network also takes that direct path, including traffic from VPC networks in your projects. Google Cloud customers must request that direct egress pricing be enabled for each of their projects after they have established Direct Peering with Google. For more information, see Pricing.

**NEW QUESTION 15**
You are deploying a global external TCP load balancing solution and want to preserve the source IP address of the original layer 3 payload.
Which type of load balancer should you use?

A. HTTP(S) load balancer
B. Network load balancer
C. Internal load balancer
D. TCP/SSL proxy load balancer

**Answer:** D

**Explanation:**
By default TCP/SSL proxy load balancer original client IP address and port information is not preserved, but it can be preserved using the PROXY protocol:
https://cloud.google.com/load-balancing/docs/tcp#target-proxies
https://medium.com/google-cloud/preserving-client-ips-through-google-clouds-global-tcp-and-ssl-proxy-load-ba

**NEW QUESTION 16**
You want to use Partner Interconnect to connect your on-premises network with your VPC. You already have an Interconnect partner.
What should you first?

A. Log in to your partner’s portal and request the VLAN attachment there.
B. Ask your Interconnect partner to provision a physical connection to Google.
C. Create a Partner Interconnect type VLAN attachment in the GCP Console and retrieve the pairing key.
D. Run gcloud compute interconnect attachments partner update <attachment> / -- region <region>--admin-enabled.

**Answer:** B

**Explanation:**
https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview?hl=En#provisionin "To provision a Partner Interconnect connection with a service provider, you start by connecting your
on-premises network to a supported service provider. Work with the service provider to establish connectivity.

**NEW QUESTION 21**
You have an application running on Compute Engine that uses BigQuery to generate some results that are stored in Cloud Storage. You want to ensure that none of the application instances have external IP addresses.
Which two methods can you use to accomplish this? (Choose two.)

A. Enable Private Google Access on all the subnets.
B. Enable Private Google Access on the VPC.
C. Enable Private Services Access on the VPC.
D. Create network peering between your VPC and BigQuery.
E. Create a Cloud NAT, and route the application traffic via NAT gateway.

**Answer:** AE

**Explanation:**
https://cloud.google.com/nat/docs/overview#interaction-pga Specifications https://cloud.google.com/vpc/docs/configure-private-google-access#specifications

**NEW QUESTION 22**
Your organization uses a Shared VPC architecture with a host project and three service projects. You have Compute Engine instances that reside in the service projects. You have critical workloads in your on-premises data center. You need to ensure that the Google Cloud instances can resolve on-premises hostnames via the Dedicated Interconnect you deployed to establish hybrid connectivity. What should you do?

A. Create a Cloud DNS private forwarding zone in the host project of the Shared VPC that forwards the private zone to the on-premises DNS servers.In your Cloud Router, add a custom route advertisement for the IP 35.199.192.0/19 to the on-premises environment.
B. Create a Cloud DNS private forwarding zone in the host project of the Shared VPC that forwards the Private zone to the on-premises DNS servers.In your Cloud Router, add a custom route advertisement for the IP 169.254 169.254 to the on-premisesenvironment.
C. Configure a Cloud DNS private zone in the host project of the Shared VPC.Set up DNS forwarding to your Google Cloud private zone on your on-premises DNS servers to point to the inbound forwarder IP address in your host projectIn your Cloud Router, add a custom route advertisement for the IP 169.254 169 254 to the on-premises environment.
D. Configure a Cloud DNS private zone in the host project of the Shared VPC.Set up DNS forwarding to your Google Cloud private zone on your on-premises DNS servers to point to the inbound forwarder IP address in your host project.Configure a DNS policy in the Shared VPC to allow inbound query forwarding with your on-

premises DNS server as the alternative DNS server.

**Answer:** D

**NEW QUESTION 24**
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.

**Answer:** C

**Explanation:**
https://cloud.google.com/load-balancing/docs/https/setting-up-https#sendtraffic

**NEW QUESTION 26**
You have created an HTTP(S) load balanced service. You need to verify that your backend instances are responding properly.
How should you configure the health check?

A. Set request-path to a specific URL used for health checking, and set proxy-header to PROXY_V1.
B. Set request-path to a specific URL used for health checking, and set host to include a custom host header that identifies the health check.
C. Set request-path to a specific URL used for health checking, and set response to a string that the backend service will always return in the response body.
D. Set proxy-header to the default value, and set host to include a custom host header that identifies the health check.

**Answer:** C

**Explanation:**
https://cloud.google.com/load-balancing/docs/health-check-concepts#content-based_health_checks

**NEW QUESTION 30**
You work for a university that is migrating to Google Cloud.
These are the cloud requirements:
On-premises connectivity with 10 Gbps Lowest latency access to the cloud Centralized Networking Administration Team
New departments are asking for on-premises connectivity to their projects. You want to deploy the most cost-efficient interconnect solution for connecting the campus to Google Cloud.
What should you do?

A. Use Shared VPC, and deploy the VLAN attachments and Dedicated Interconnect in the host project.
B. Use Shared VPC, and deploy the VLAN attachments in the service project
C. Connect the VLAN attachment to the Shared VPC's host project.
D. Use standalone projects, and deploy the VLAN attachments in the individual project
E. Connect the VLAN attachment to the standalone projects' Dedicated Interconnects.
F. Use standalone projects and deploy the VLAN attachments and Dedicated Interconnects in each of the individual projects.

**Answer:** A

**NEW QUESTION 35**
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?

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

**NEW QUESTION 40**
Your company has a Virtual Private Cloud (VPC) with two Dedicated Interconnect connections in two different regions: us-west1 and us-east1. Each Dedicated Interconnect connection is attached to a Cloud Router in its respective region by a VLAN attachment. You need to configure a high availability failover path. By default, all ingress traffic from the on-premises environment should flow to the VPC using the us-west1 connection. If us-west1 is unavailable, you want traffic to be rerouted to us-east1. How should you configure the multi-exit discriminator (MED) values to enable this failover path?

A. Use regional routin
B. Set the us-east1 Cloud Router to a base priority of 100, and set the us-west1 CloudRouter to a base priority of 1
C. Use global routin
D. Set the us-east1 Cloud Router to a base priority of 100, and set the us-west1 Cloud Router to a base priority of 1
E. Use regional routin
F. Set the us-east1 Cloud Router to a base priority of 1000, and set the us-west1 Cloud Router to a base priority of 1
G. Use global routin
H. Set the us-east1 Cloud Router to a base priority of 1000, and set the us-west1 Cloud Router to a base priority of 1

**Answer:** A

**NEW QUESTION 44**
You have provisioned a Partner Interconnect connection to extend connectivity from your on-premises data center to Google Cloud. You need to configure a Cloud Router and create a VLAN attachment to connect to resources inside your VPC. You need to configure an Autonomous System number (ASN) to use with the associated Cloud Router and create the VLAN attachment.
What should you do?

A. Use a 4-byte private ASN 4200000000-4294967294.
B. Use a 2-byte private ASN 64512-65535.
C. Use a public Google ASN 15169.
D. Use a public Google ASN 16550.

**Answer:** B

**NEW QUESTION 49**
You are creating an instance group and need to create a new health check for HTTP(s) load balancing. Which two methods can you use to accomplish this? (Choose two.)

A. Create a new health check using the gcloud command line tool.
B. Create a new health check using the VPC Network section in the GCP Console.
C. Create a new health check, or select an existing one, when you complete the load balancer's backend configuration in the GCP Console.
D. Create a new legacy health check using the gcloud command line tool.
E. Create a new legacy health check using the Health checks section in the GCP Console.

**Answer:** AC

**Explanation:**
https://cloud.google.com/load-balancing/docs/health-checks#creating_and_modifying_health_checks

**NEW QUESTION 52**
You are migrating to Cloud DNS and want to import your BIND zone file. Which command should you use?

A. gcloud dns record-sets import ZONE_FILE --zone MANAGED_ZONE
B. gcloud dns record-sets import ZONE_FILE --replace-origin-ns --zone MANAGED_ZONE
C. gcloud dns record-sets import ZONE_FILE --zone-file-format --zone MANAGED_ZONE
D. gcloud dns record-sets import ZONE_FILE --delete-all-existing --zone MANAGED ZONE

**Answer:** C

**Explanation:**
https://cloud.google.com/sdk/gcloud/reference/dns/record-sets/import

**NEW QUESTION 54**
You are configuring a new HTTP application that will be exposed externally behind both IPv4 and IPv6 virtual IP addresses, using ports 80, 8080, and 443. You will have backends in two regions: us-west1 and
us-east1. You want to serve the content with the lowest-possible latency while ensuring high availability and autoscaling, and create native content-based rules using the HTTP hostname and request path. The IP addresses of the clients that connect to the load balancer need to be visible to the backends. Which configuration should you use?

A. Use Network Load Balancing
B. Use TCP Proxy Load Balancing with PROXY protocol enabled
C. Use External HTTP(S) Load Balancing with URL Maps and custom headers
D. Use External HTTP(S) Load Balancing with URL Maps and an X-Forwarded-For header

**Answer:** D

**NEW QUESTION 55**
You suspect that one of the virtual machines (VMs) in your default Virtual Private Cloud (VPC) is under a denial-of-service attack. You need to analyze the incoming traffic for the VM to understand where the traffic is coming from. What should you do?

A. Enable Data Access audit logs of the VP
B. Analyze the logs and get the source IP addresses from the subnetworks.get field.
C. Enable VPC Flow Logs for the subne
D. Analyze the logs and get the source IP addresses from the connection field.
E. Enable VPC Flow Logs for the VP
F. Analyze the logs and get the source IP addresses from the src_location field.
G. Enable Data Access audit logs of the subne
H. Analyze the logs and get the source IP addresses from the networks.get field.

**Answer:** B

**NEW QUESTION 56**
Your company is working with a partner to provide a solution for a customer. Both your company and the partner organization are using GCP. There are applications in the partner's network that need access to some resources in your company's VPC. There is no CIDR overlap between the VPCs.
Which two solutions can you implement to achieve the desired results without compromising the security? (Choose two.)

A. VPC peering
B. Shared VPC
C. Cloud VPN
D. Dedicated Interconnect
E. Cloud NAT

**Answer:** AC

**Explanation:**
Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization.

**NEW QUESTION 61**
Your end users are located in close proximity to us-east1 and europe-west1. Their workloads need to communicate with each other. You want to minimize cost and increase network efficiency.
How should you design this topology?

A. Create 2 VPCs, each with their own regions and individual subnet
B. Create 2 VPN gateways to establish connectivity between these regions.
C. Create 2 VPCs, each with their own region and individual subnet
D. Use external IP addresses on the instances to establish connectivity between these regions.
E. Create 1 VPC with 2 regional subnet
F. Create a global load balancer to establish connectivity between the regions.
G. Create 1 VPC with 2 regional subnet
H. Deploy workloads in these subnets and have them communicate using private RFC1918 IP addresses.

**Answer:** D

**Explanation:**
https://cloud.google.com/vpc/docs/using-vpc#create-auto-network
We create one VPC network in auto mode that creates one subnet in each Google Cloud region automatically. So, region us-east1 and europe-west1 are in the same network and they can communicate using their internal IP address even though they are in different Regions. They take advantage of Google's global fiber network.

**NEW QUESTION 63**
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?

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 hu
B. Import the custom routes in the spokes.
C. 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 hu
D. Import the custom routes in the spoke
E. Delete the default internet gateway route of the spokes.
F. 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 hu
G. Import the custom routes in the spokes.
H. 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

**NEW QUESTION 67**
Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from your on-premises network using Cloud Interconnect. You must configure access only to Google APIs and services that are supported by VPC Service Controls through hybrid connectivity with a service level agreement (SLA) in place. What should you do?

A. Configure the existing Cloud Routers to advertise the Google API's public virtual IP addresses.
B. Use Private Google Access for on-premises hosts with restricted.googleapis.com virtual IP addresses.
C. Configure the existing Cloud Routers to advertise a default route, and use Cloud NAT to translate traffic from your on-premises network.
D. Add Direct Peering links, and use them for connectivity to Google APIs that use public virtual IP addresses.

**Answer:** B

**NEW QUESTION 70**
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 have recently engaged a traffic-scrubbing service and want to restrict your origin to allow connections only from the traffic-scrubbing service.
What should you do?

A. Create a Cloud Armor Security Policy that blocks all traffic except for the traffic-scrubbing service.
B. Create a VPC Firewall rule that blocks all traffic except for the traffic-scrubbing service.
C. Create a VPC Service Control Perimeter that blocks all traffic except for the traffic-scrubbing service.
D. Create IPTables firewall rules that block all traffic except for the traffic-scrubbing service.

**Answer:** A

**Explanation:**
Global load balancer will proxy the connection . thus no trace of session origin IP. you should use Cloud Armor to geofence your service.
https://cloud.google.com/load-balancing/docs/https

**NEW QUESTION 73**
You need to establish network connectivity between three Virtual Private Cloud networks, Sales, Marketing, and Finance, so that users can access resources in all three VPCs. You configure VPC peering between the Sales VPC and the Finance VPC. You also configure VPC peering between the Marketing VPC and the Finance VPC. After you complete the configuration, some users cannot connect to resources in the Sales VPC and the Marketing VPC. You want to resolve the problem.
What should you do?

A. Configure VPC peering in a full mesh.
B. Alter the routing table to resolve the asymmetric route.
C. Create network tags to allow connectivity between all three VPCs.
D. Delete the legacy network and recreate it to allow transitive peering.

**Answer:** A

**Explanation:**
https://cloud.google.com/vpc/docs/using-vpc-peering

**NEW QUESTION 74**
You have the following private Google Kubernetes Engine (GKE) cluster deployment:

```
gcloud container clusters describe customer-1-cluster --zone us-central1-c

...

clusterIpv4Cidr: 192.168.36.0/24
endpoint: 192.168.38.2
ipAllocationPolicy:
  clusterIpv4Cidr: 192.168.36.0/24
  clusterIpv4CidrBlock: 192.168.36.0/24
  clusterSecondaryRangeName: customer-1-pods
  servicesIpv4Cidr: 192.168.37.0/24
  servicesIp4CidrBlock: 192.168.37.0/24
  servicesSecondaryRangeName: customer-1-svc
  useIpAliases: true

...

masterAuthorizedNetworksConfig:

...

privateClusterConfig:
  enablePrivateEndpoint: true
  enablePrivateNodes: true
  masterIpv4CidrBlock: 192.168.38.0/28
  privateEndpoint: 192.168.38.2
  publicEndpoint: 35.224.37.17

...

servicesIpv4Cidr: 192.162.37.0/24

...

subnetwork: customer-1-nodes
zone: us-central1-c
```

You have a virtual machine (VM) deployed in the same VPC in the subnetwork kubernetes-management with internal IP address 192.168.40 2/24 and no external

IP address assigned. You need to communicate with the cluster master using kubectl. What should you do?

A. Add the network 192.168.40.0/24 to the masterAuthorizedNetworksConfi
B. Configure kubectl tocommunicate with the endpoint 192.168.38.2.
C. Add the network 192.168.38.0/28 to the masterAuthorizedNetworksConfi
D. Configure kubectl to communicate with the endpoint 192.168.38.2
E. Add the network 192.168.36.0/24 to the masterAuthorizedNetworksConfi
F. Configure kubectl to communicate with the endpoint 192.168.38.2
G. Add an external IP address to the VM, and add this IP address in the masterAuthorizedNetworksConfig.Configure kubectl to communicate with the endpoint 35.224.37.17.

**Answer:** A

**NEW QUESTION 79**
After a network change window one of your company's applications stops working. The application uses an on-premises database server that no longer receives any traffic from the application. The database server IP address is 10.2.1.25. You examine the change request, and the only change is that 3 additional VPC subnets were created. The new VPC subnets created are 10.1.0.0/16, 10.2.0.0/16, and 10.3.1.0/24/ The on-premises router is advertising 10.0.0.0/8.
What is the most likely cause of this problem?

A. The less specific VPC subnet route is taking priority.
B. The more specific VPC subnet route is taking priority.
C. The on-premises router is not advertising a route for the database server.
D. A cloud firewall rule that blocks traffic to the on-premises database server was created during the change.

**Answer:** B

**NEW QUESTION 81**
You work for a multinational enterprise that is moving to GCP. These are the cloud requirements:
• An on-premises data center located in the United States in Oregon and New York with Dedicated Interconnects connected to Cloud regions us-west1 (primary HQ) and us-east4 (backup)
• Multiple regional offices in Europe and APAC
• Regional data processing is required in europe-west1 and australia-southeast1
• Centralized Network Administration Team
Your security and compliance team requires a virtual inline security appliance to perform L7 inspection for URL filtering. You want to deploy the appliance in us-west1.
What should you do?

A. • Create 2 VPCs in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Host Project.• Attach NIC0 in VPC #1 us-west1 subnet of the Host Project.• Attach NIC1 in VPC #2 us-west1 subnet of the Host Project.• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.
B. • Create 2 VPCs in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Service Project.• Attach NIC0 in VPC #1 us-west1 subnet of the Host Project.• Attach NIC1 in VPC #2 us-west1 subnet of the Host Project.• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.
C. • Create 1 VPC in a Shared VPC Host Project.• Configure a 2-NIC instance in zone us-west1-a in the Host Project.• Attach NIC0 in us-west1 subnet of the Host Project.• Attach NIC1 in us-west1 subnet of the Host Project• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.
D. • Create 1 VPC in a Shared VPC Service Project.• Configure a 2-NIC instance in zone us-west1-a in the Service Project.• Attach NIC0 in us-west1 subnet of the Service Project.• Attach NIC1 in us-west1 subnet of the Service Project• Deploy the instance.• Configure the necessary routes and firewall rules to pass traffic through the instance.

**Answer:** B

**Explanation:**
https://cloud.google.com/vpc/docs/shared-vpc

**NEW QUESTION 86**
You deployed a hub-and-spoke architecture in your Google Cloud environment that uses VPC Network Peering to connect the spokes to the hub. For security reasons, you deployed a private Google Kubernetes
Engine (GKE) cluster in one of the spoke projects with a private endpoint for the control plane. You configured authorized networks to be the subnet range where the GKE nodes are deployed. When you attempt to reach the GKE control plane from a different spoke project, you cannot access it. You need to allow access to the GKE control plane from the other spoke projects. What should you do?

A. Add a firewall rule that allows port 443 from the other spoke projects.
B. Enable Private Google Access on the subnet where the GKE nodes are deployed.
C. Configure the authorized networks to be the subnet ranges of the other spoke projects.
D. Deploy a proxy in the spoke project where the GKE nodes are deployed and connect to the control plane through the proxy.

**Answer:** C

**NEW QUESTION 88**
You are designing a shared VPC architecture. Your network and security team has strict controls over which routes are exposed between departments. Your Production and Staging departments can communicate with each other, but only via specific networks. You want to follow Google-recommended practices.
How should you design this topology?

A. Create 2 shared VPCs within the shared VPC Host Project, and enable VPC peering between the
B. Use firewall rules to filter access between the specific networks.
C. Create 2 shared VPCs within the shared VPC Host Project, and create a Cloud VPN/Cloud Router between the
D. Use Flexible Route Advertisement (FRA) to filter access between the specific networks.
E. Create 2 shared VPCs within the shared VPC Service Project, and create a Cloud VPN/Cloud Router between the

F. Use Flexible Route Advertisement (FRA) to filter access between the specific networks.
G. Create 1 VPC within the shared VPC Host Project, and share individual subnets with the Service Projects to filter access between the specific networks.

**Answer:** D

**NEW QUESTION 91**
You create multiple Compute Engine virtual machine instances to be used as TFTP servers. Which type of load balancer should you use?

A. HTTP(S) load balancer
B. SSL proxy load balancer
C. TCP proxy load balancer
D. Network load balancer

**Answer:** D

**Explanation:**
"TFTP is a UDP-based protocol. Servers listen on port 69 for the initial client-to-server packet to establish the TFTP session, then use a port above 1023 for all further packets during that session. Clients use ports above 1023" https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch17_02.htm Besides, Google Cloud external TCP/UDP Network Load Balancing (after this referred to as Network Load Balancing) is a regional,
non-proxied load balancer. Network Load Balancing distributes traffic among virtual machine (VM) instances in the same region in a Virtual Private Cloud (VPC) netw

**NEW QUESTION 96**
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?

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

**NEW QUESTION 99**
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.

**Answer:** A

**NEW QUESTION 101**
Your organization is implementing a new security policy to control how firewall rules are applied to control flows between virtual machines (VMs). Using Google-recommended practices, you need to set up a firewall rule to enforce strict control of traffic between VM A and VM B. You must ensure that communications flow only from VM A to VM B within the VPC, and no other communication paths are allowed. No other firewall rules exist in the VPC. Which firewall rule should you configure to allow only this communication path?

A. Firewall rule direction: ingress Action: allowTarget: VM B service accountSource ranges: VM A service account Priority: 1000
B. Firewall rule direction: ingress Action: allowTarget: specific VM B tagSource ranges: VM A tag and VM A source IP address Priority: 1000
C. Firewall rule direction: ingress Action: allowTarget: VM A service accountSource ranges: VM B service account and VM B source IP address Priority: 100
D. Firewall rule direction: ingress Action: allowTarget: specific VM A tagSource ranges: VM B tag and VM B source IP address Priority: 100

**Answer:** D

**NEW QUESTION 102**
Your organization has a new security policy that requires you to monitor all egress traffic payloads from your virtual machines in region us-west2. You deployed an intrusion detection system (IDS) virtual appliance in the same region to meet the new policy. You now need to integrate the IDS into the environment to monitor all egress traffic payloads from us-west2. What should you do?

A. Enable firewall logging, and forward all filtered egress firewall logs to the IDS.
B. Enable VPC Flow Log
C. Create a sink in Cloud Logging to send filtered egress VPC Flow Logs to the IDS.
D. Create an internal TCP/UDP load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.
E. Create an internal HTTP(S) load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.

**Answer:** B

**NEW QUESTION 103**
You are configuring an HA VPN connection between your Virtual Private Cloud (VPC) and on-premises network. The VPN gateway is named VPN_GATEWAY_1. You need to restrict VPN tunnels created in the project to only connect to your on-premises VPN public IP address: 203.0.113.1/32. What should you do?

A. Configure a firewall rule accepting 203.0.113.1/32, and set a target tag equal to VPN_GATEWAY_1.
B. Configure the Resource Manager constraint constraints/compute.restrictVpnPeerIPs to use an allowList consisting of only the 203.0.113.1/32 address.

C. Configure a Google Cloud Armor security policy, and create a policy rule to allow 203.0.113.1/32.
D. Configure an access control list on the peer VPN gateway to deny all traffic except 203.0.113.1/32, and attach it to the primary external interface.

**Answer:** B

**NEW QUESTION 104**
You are using the gcloud command line tool to create a new custom role in a project by coping a predefined role. You receive this error message: INVALID_ARGUMENT: Permission resourcemanager.projects.list is not valid What should you do?

A. Add the resourcemanager.projects.get permission, and try again.
B. Try again with a different role with a new name but the same permissions.
C. Remove the resourcemanager.projects.list permission, and try again.
D. Add the resourcemanager.projects.setIamPolicy permission, and try again.

**Answer:** C

**NEW QUESTION 108**
Your company has 10 separate Virtual Private Cloud (VPC) networks, with one VPC per project in a single region in Google Cloud. Your security team requires each VPC network to have private connectivity to the main on-premises location via a Partner Interconnect connection in the same region. To optimize cost and operations, the same connectivity must be shared with all projects. You must ensure that all traffic between different projects, on-premises locations, and the internet can be inspected using the same third-party appliances. What should you do?

A. Configure the third-party appliances with multiple interfaces and specific Partner Interconnect VLAN attachments per projec
B. Create the relevant routes on the third-party appliances and VPC networks.
C. Configure the third-party appliances with multiple interfaces, with each interface connected to a separate VPC networ
D. Create separate VPC networks for on- premises and internet connectivit
E. Create the relevant routes on the third-party appliances and VPC networks.
F. Consolidate all existing projects' subnetworks into a single VP
G. Create separate VPC networks for on-premises and internet connectivit
H. Configure the third-party appliances with multiple interfaces, with each interface connected to a separate VPC networ
I. Create the relevant routes on the third-party appliances and VPC networks.
J. Configure the third-party appliances with multiple interface
K. Create a hub VPC network for all projects, and create separate VPC networks for on-premises and internet connectivit
L. Create the relevant routes on the third-party appliances and VPC network
M. Use VPC Network Peering to connect all projects' VPC networks to the hub VP
N. Export custom routes from the hub VPC and import on all projects' VPC networks.

**Answer:** D

**NEW QUESTION 111**
You are designing a Partner Interconnect hybrid cloud connectivity solution with geo-redundancy across two metropolitan areas. You want to follow Google-recommended practices to set up the following region/metro pairs:
(region 1/metro 1)
(region 2/metro 2) What should you do?

A. Create a Cloud Router in region 1 with two VLAN attachments connected to metro1-zone1-x.Create a Cloud Router in region 2 with two VLAN attachments connected to metro1-zone2-x.
B. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone1-x.Create a Cloud Router in region 2 with two VLAN attachments connected to metro2-zone2-x.
C. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone2-x.Create a Cloud Router in region 2 with one VLAN attachment connected to metro2-zone2-x.
D. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone1-x and one VLAN attachment connected to metro1-zone2-x.Create a Cloud Router in region 2 with one VLAN attachment connected to metro2-zone1-x and one VLAN attachment to metro2-zone2-x.

**Answer:** B

**NEW QUESTION 112**
You recently configured Google Cloud Armor security policies to manage traffic to your application. You discover that Google Cloud Armor is incorrectly blocking some traffic to your application. You need to identity the web application firewall (WAF) rule that is incorrectly blocking traffic. What should you do?

A. Enable firewall logs, and view the logs in Firewall Insights.
B. Enable HTTP(S) Load Balancing logging with sampling rate equal to 1, and view the logs in Cloud Logging.
C. Enable VPC Flow Logs, and view the logs in Cloud Logging.
D. Enable Google Cloud Armor audit logs, and view the logs on the Activity page in the Google CloudConsole.

**Answer:** A

**NEW QUESTION 116**
You are adding steps to a working automation that uses a service account to authenticate. You need to drive the automation the ability to retrieve files from a Cloud Storage bucket. Your organization requires using the least privilege possible.
What should you do?

A. Grant the compute.instanceAdmin to your user account.
B. Grant the iam.serviceAccountUser to your user account.
C. Grant the read-only privilege to the service account for the Cloud Storage bucket.
D. Grant the cloud-platform privilege to the service account for the Cloud Storage bucket.

**Answer:** C

**NEW QUESTION 120**
You need to configure a static route to an on-premises resource behind a Cloud VPN gateway that is configured for policy-based routing using the gcloud command.
Which next hop should you choose?

A. The default internet gateway
B. The IP address of the Cloud VPN gateway
C. The name and region of the Cloud VPN tunnel
D. The IP address of the instance on the remote side of the VPN tunnel

**Answer:** C

**Explanation:**
When you create a route based tunnel using the Cloud Console, Classic VPN performs both of the following tasks: Sets the tunnel's local and remote traffic selectors to any IP address (0.0.0.0/0) For each range in Remote network IP ranges, Google Cloud creates a custom static route whose destination (prefix) is the range's CIDR, and whose next hop is the tunnel.
https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns

**NEW QUESTION 124**
You have recently been put in charge of managing identity and access management for your organization. You have several projects and want to use scripting and automation wherever possible. You want to grant the editor role to a project member.
Which two methods can you use to accomplish this? (Choose two.)

A. GetIamPolicy() via REST API
B. setIamPolicy() via REST API
C. gcloud pubsub add-iam-policy-binding Sprojectname --member user:Susername --role roles/editor
D. gcloud projects add-iam-policy-binding Sprojectname --member user:Susername --role roles/editor
E. Enter an email address in the Add members field, and select the desired role from the drop-down menu in the GCP Console.

**Answer:** DE

**NEW QUESTION 128**
Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from on-premises locations using Cloud Interconnect connections. Your company must be able to send traffic to Cloud Storage only through the Interconnect links while accessing other Google APIs and services over the public internet. What should you do?

A. Use the default public domains for all Google APIs and services.
B. Use Private Service Connect to access Cloud Storage, and use the default public domains for all other Google APIs and services.
C. Use Private Google Access, with restricted.googleapis.com virtual IP addresses for Cloud Storage and private.googleapis.com for all other Google APIs and services.
D. Use Private Google Access, with private.googleapis.com virtual IP addresses for Cloud Storage and restricted.googleapis.com virtual IP addresses for all other Google APIs and services.

**Answer:** B

**NEW QUESTION 133**
You want to set up two Cloud Routers so that one has an active Border Gateway Protocol (BGP) session, and the other one acts as a standby.
Which BGP attribute should you use on your on-premises router?

A. AS-Path
B. Community
C. Local Preference
D. Multi-exit Discriminator

**Answer:** D

**NEW QUESTION 136**
Your company has separate Virtual Private Cloud (VPC) networks in a single region for two departments: Sales and Finance. The Sales department's VPC network already has connectivity to on-premises locations using HA VPN, and you have confirmed that the subnet ranges do not overlap. You plan to peer both VPC networks to use the same HA tunnels for on-premises connectivity, while providing internet connectivity for the Google Cloud workloads through Cloud NAT. Internet access from the on-premises locations should not flow through Google Cloud. You need to propagate all routes between the Finance department and on-premises locations. What should you do?

A. Peer the two VPCs, and use the default configuration for the Cloud Routers.
B. Peer the two VPCs, and use Cloud Router’s custom route advertisements to announce the peered VPC network ranges to the on-premises locations.
C. Peer the two VPC
D. Configure VPC Network Peering to export custom routes from Sales and import custom routes on Finance's VPC networ
E. Use Cloud Router’s custom route advertisements to announce a default route to the on-premises locations.
F. Peer the two VPC
G. Configure VPC Network Peering to export custom routes from Sales and import custom routes on Finance's VPC networ
H. Use Cloud Router’s custom route advertisements to announce the peered VPC network ranges to the on-premises locations.

**Answer:** A

**NEW QUESTION 140**
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

**Answer:** C

**NEW QUESTION 142**
You are the Organization Admin for your company. One of your engineers is responsible for setting up multiple host projects across multiple folders and sharing subnets with service projects. You need to enable the engineer's Identity and Access Management (IAM) configuration to complete their task in the fewest number of steps. What should you do?

A. Set up the engineer with Compute Shared VPC Admin IAM role at the folder level.
B. Set up the engineer with Compute Shared VPC Admin IAM role at the organization level.
C. Set up the engineer with Compute Shared VPC Admin IAM role and Project IAM Admin role at the folder level.
D. Set up the engineer with Compute Shared VPC Admin IAM role and Project IAM Admin role at the organization level.

**Answer:** B

**NEW QUESTION 145**
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:
• Flow logs are enabled for the VPC subnet, and all firewall rules are set to log.
• The subnetwork logs are not excluded from Stackdriver.
• The instance that is hosting the application can communicate outside the subnet.
• Other instances within the subnet can communicate outside the subnet.
• 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.

**Answer:** C

**NEW QUESTION 148**
You need to create a GKE cluster in an existing VPC that is accessible from on-premises. You must meet the following requirements:
- IP ranges for pods and services must be as small as possible.
- The nodes and the master must not be reachable from the internet.
- You must be able to use kubectl commands from on-premises subnets to manage the cluster.

How should you create the GKE cluster?

A. • Create a private cluster that uses VPC advanced routes.•Set the pod and service ranges as /24.•Set up a network proxy to access the master.
B. • Create a VPC-native GKE cluster using GKE-managed IP ranges.•Set the pod IP range as /21 and service IP range as /24.•Set up a network proxy to access the master.
C. • Create a VPC-native GKE cluster using user-managed IP ranges.•Enable a GKE cluster network policy, set the pod and service ranges as /24.•Set up a network proxy to access the master.•Enable master authorized networks.
D. • Create a VPC-native GKE cluster using user-managed IP ranges.•Enable privateEndpoint on the cluster master.•Set the pod and service ranges as /24.•Set up a network proxy to access the master.•Enable master authorized networks.

**Answer:** D

**Explanation:**
Creating GKE private clusters with network proxies for controller access When you create a GKE private cluster with a private cluster controller endpoint, the cluster's controller node is inaccessible from the public internet, but it needs to be accessible for administration. By default, clusters can access the controller through its private endpoint, and authorized networks can be defined within the VPC network. To access the controller from on-premises or another VPC network, however, requires additional steps. This is because the VPC network that hosts the controller is owned by Google and cannot be accessed from resources connected through another VPC network peering connection, Cloud VPN or Cloud Interconnect. https://cloud.google.com/solutions/creating-kubernetes-engine-private-clusters-with-net-proxies

**NEW QUESTION 153**
Your company’s on-premises network is connected to a VPC using a Cloud VPN tunnel. You have a static route of 0.0.0.0/0 with the VPN tunnel as its next hop defined in the VPC. All internet bound traffic currently passes through the on-premises network. You configured Cloud NAT to translate the primary IP addresses of Compute Engine instances in one region. Traffic from those instances will now reach the internet directly from their VPC and not from the on-premises network. Traffic from the virtual machines (VMs) is not translating addresses as expected. What should you do?

A. Lower the TCP Established Connection Idle Timeout for the NAT gateway.
B. Add firewall rules that allow ingress and egress of the external NAT IP address, have a target tag that is on the Compute Engine instances, and have a priority value higher than the priority value of the default route to the VPN gateway.
C. Add a default static route to the VPC with the default internet gateway as the next hop, the network tag associated with the Compute Engine instances, and a higher priority than the priority of the default route to the VPN tunnel.
D. Increase the default min-ports-per-vm setting for the Cloud NAT gateway.

**Answer:** A

**NEW QUESTION 154**
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 172.16.45.0/24network.

**Answer:** C

**NEW QUESTION 156**
You have configured a Compute Engine virtual machine instance as a NAT gateway. You execute the following command:
gcloud compute routes create no-ip-internet-route \
--network custom-network1 \
--destination-range 0.0.0.0/0 \
--next-hop instance nat-gateway \
--next-hop instance-zone us-central1-a \
--tags no-ip --priority 800
You want existing instances to use the new NAT gateway. Which command should you execute?

A. sudo sysctl -w net.ipv4.ip_forward=1
B. gcloud compute instances add-tags [existing-instance] --tags no-ip
C. gcloud builds submit --config=cloudbuild.waml --substitutions=TAG_NAME=no-ip
D. gcloud compute instances create example-instance --network custom-network1 \--subnet subnet-us-central \--no-address \--zone us-central1-a \--image-family debian-9 \--image-project debian-cloud \--tags no-ip

**Answer:** B

**Explanation:**
https://cloud.google.com/sdk/gcloud/reference/compute/routes/create
In order to apply a route to an existing instance we should use a tag to bind the route to it.

**NEW QUESTION 157**
You need to ensure your personal SSH key works on every instance in your project. You want to accomplish this as efficiently as possible.
What should you do?

A. Upload your public ssh key to the project Metadata.
B. Upload your public ssh key to each instance Metadata.
C. Create a custom Google Compute Engine image with your public ssh key embedded.
D. Use gcloud compute ssh to automatically copy your public ssh key to the instance.

**Answer:** A

**Explanation:**
Overview By creating and managing SSH keys, you can let users access a Linux instance through third-party tools. An SSH key consists of the following files: A public SSH key file that is applied to instance-level metadata or project-wide metadata. A private SSH key file that the user stores on their local devices. If a user presents their private SSH key, they can use a third-party tool to connect to any instance that is configured with the matching public SSH key file, even if they aren't a member of your Google Cloud project. Therefore, you can control which instances a user can access by changing the public SSH key metadata for one or more instances. https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#addkey

**NEW QUESTION 161**
You have provisioned a Dedicated Interconnect connection of 20 Gbps with a VLAN attachment of 10 Gbps. You recently noticed a steady increase in ingress traffic on the Interconnect connection from the on-premises data center. You need to ensure that your end users can achieve the full 20 Gbps throughput as quickly as possible. Which two methods can you use to accomplish this? (Choose two.)

A. Configure an additional VLAN attachment of 10 Gbps in another regio
B. Configure the on-premises router to advertise routes with the same multi-exit discriminator (MED).
C. Configure an additional VLAN attachment of 10 Gbps in the same regio
D. Configure the on-premises router to advertise routes with the same multi-exit discriminator (MED).
E. From the Google Cloud Console, modify the bandwidth of the VLAN attachment to 20 Gbps.
F. From the Google Cloud Console, request a new Dedicated Interconnect connection of 20 Gbps, and configure a VLAN attachment of 10 Gbps.
G. Configure Link Aggregation Control Protocol (LACP) on the on-premises router to use the 20-Gbps Dedicated Interconnect connection.

**Answer:** CE

**NEW QUESTION 162**
.....

# Thank You for Trying Our Product

## We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

## Professional-Cloud-Network-Engineer Practice Exam Features:

* Professional-Cloud-Network-Engineer Questions and Answers Updated Frequently

* Professional-Cloud-Network-Engineer Practice Questions Verified by Expert Senior Certified Staff

* Professional-Cloud-Network-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* Professional-Cloud-Network-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year