

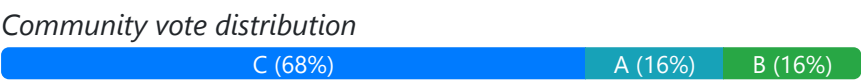
Topic 1 - Single Topic

Question #1 Topic 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



Question #2 Topic 1

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

Correct Answer: D



Question #3 Topic 1

Your organization is deploying a single project for 3 separate departments. Two of these departments require network connectivity between each other, but the third department should remain in isolation. Your design should create separate network administrative domains between these departments. You want to minimize operational overhead. How should you design the topology?

- A. Create a Shared VPC Host Project and the respective Service Projects for each of the 3 separate departments.
- B. Create 3 separate VPCs, and use Cloud VPN to establish connectivity between the two appropriate VPCs.
- C. Create 3 separate VPCs, and use VPC peering to establish connectivity between the two appropriate VPCs.
- D. Create a single project, and deploy specific firewall rules. Use network tags to isolate access between the departments.

Correct Answer: C

Community vote distribution



Question #4 Topic 1

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

Correct Answer: C

Community vote distribution



Topic 1 - Single Topic

Question #1 Topic 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

Community vote distribution



Question #2 Topic 1

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

Correct Answer: D

Community vote distribution



Question #3 Topic 1

Your organization is deploying a single project for 3 separate departments. Two of these departments require network connectivity between each other, but the third department should remain in isolation. Your design should create separate network administrative domains between these departments. You want to minimize operational overhead. How should you design the topology?

- A. Create a Shared VPC Host Project and the respective Service Projects for each of the 3 separate departments.
- B. Create 3 separate VPCs, and use Cloud VPN to establish connectivity between the two appropriate VPCs.
- C. Create 3 separate VPCs, and use VPC peering to establish connectivity between the two appropriate VPCs.
- D. Create a single project, and deploy specific firewall rules. Use network tags to isolate access between the departments.

Correct Answer: C

Community vote distribution



Question #4 Topic 1

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

Correct Answer: C

Community vote distribution



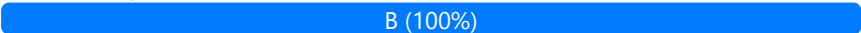
Question #5 Topic 1

You created a VPC network named Retail in auto mode. You want to create a VPC network named Distribution and peer it with the Retail VPC. How should you configure the Distribution VPC?

- A. Create the Distribution VPC in auto mode. Peer both the VPCs via network peering.
- B. Create the Distribution VPC in custom mode. Use the CIDR range 10.0.0.0/9. Create the necessary subnets, and then peer them via network peering.
- C. Create the Distribution VPC in custom mode. Use the CIDR range 10.128.0.0/9. Create the necessary subnets, and then peer them via network peering.
- D. Rename the default VPC as "Distribution" and peer it via network peering.

Correct Answer: B

Community vote distribution



Question #6 Topic 1

You are using a third-party next-generation firewall to inspect traffic. You created a custom route of 0.0.0.0/0 to route egress traffic to the firewall. You want to allow your VPC instances without public IP addresses to access the BigQuery and Cloud Pub/Sub APIs, without sending the traffic through the firewall.

Which two actions should you take? (Choose two.)

- A. Turn on Private Google Access at the subnet level.
- B. Turn on Private Google Access at the VPC level.
- C. Turn on Private Services Access at the VPC level.
- D. Create a set of custom static routes to send traffic to the external IP addresses of Google APIs and services via the default internet gateway.
- E. Create a set of custom static routes to send traffic to the internal IP addresses of Google APIs and services via the default internet gateway.

Correct Answer: AD

Community vote distribution



Question #7 Topic 1

All the instances in your project are configured with the custom metadata enable-oslogin value set to FALSE and to block project-wide SSH keys. None of the instances are set with any SSH key, and no project-wide SSH keys have been configured. Firewall rules are set up to allow SSH sessions from any IP address range. You want to SSH into one instance.

What should you do?

- A. Open the Cloud Shell SSH into the instance using `gcloud compute ssh`.
- B. Set the custom metadata enable-oslogin to TRUE, and SSH into the instance using a third-party tool like putty or ssh.
- C. Generate a new SSH key pair. Verify the format of the private key and add it to the instance. SSH into the instance using a third-party tool like putty or ssh.
- D. Generate a new SSH key pair. Verify the format of the public key and add it to the project. SSH into the instance using a third-party tool like putty or ssh.

Correct Answer: A

Community vote distribution



Question #8 Topic 1

You work for a university that is migrating to GCP.

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

Correct Answer: A

Community vote distribution

Question #9 Topic 1

You have deployed a new internal application that provides HTTP and TFTP services to on-premises hosts. You want to be able to distribute traffic across multiple

Compute Engine instances, but need to ensure that clients are sticky to a particular instance across both services.

Which session affinity should you choose?

- A. None
- B. Client IP
- C. Client IP and protocol
- D. Client IP, port and protocol

Correct Answer: B

Community vote distribution

B (69%)

D (31%)

Question #10 Topic 1

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.

Correct Answer: D

Community vote distribution

D (85%)

Other

Question #11 Topic 1

You are trying to update firewall rules in a shared VPC for which you have been assigned only Network Admin permissions. You cannot modify the firewall rules.

Your organization requires using the least privilege necessary.

Which level of permissions should you request?

- A. Security Admin privileges from the Shared VPC Admin.
- B. Service Project Admin privileges from the Shared VPC Admin.
- C. Shared VPC Admin privileges from the Organization Admin.
- D. Organization Admin privileges from the Organization Admin.

Correct Answer: A

Community vote distribution

A (100%)

Question #12 Topic 1

You want to create a service in GCP using IPv6.
What should you do?

- A. Create the instance with the designated IPv6 address.
- B. Configure a TCP Proxy with the designated IPv6 address.
- C. Configure a global load balancer with the designated IPv6 address.
- D. Configure an internal load balancer with the designated IPv6 address.

Correct Answer: C

Community vote distribution



Question #13 Topic 1

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: B

Community vote distribution



Question #14 Topic 1

Your company just completed the acquisition of Altostrat (a current GCP customer). Each company has a separate organization in GCP and has implemented a custom DNS solution. Each organization will retain its current domain and host names until after a full transition and architectural review is done in one year.

These are the assumptions for both GCP environments.

"⌘ Each organization has enabled full connectivity between all of its projects by using Shared VPC.

"⌘ Both organizations strictly use the 10.0.0.0/8 address space for their instances, except for bastion hosts (for accessing the instances) and load balancers for serving web traffic.

"⌘ There are no prefix overlaps between the two organizations.

"⌘ Both organizations already have firewall rules that allow all inbound and outbound traffic from the 10.0.0.0/8 address space.

"⌘ Neither organization has Interconnects to their on-premises environment.

You want to integrate networking and DNS infrastructure of both organizations as quickly as possible and with minimal downtime.
Which two steps should you take? (Choose two.)

- A. Provision Cloud Interconnect to connect both organizations together.
- B. Set up some variant of DNS forwarding and zone transfers in each organization.
- C. Connect VPCs in both organizations using Cloud VPN together with Cloud Router.
- D. Use Cloud DNS to create A records of all VMs and resources across all projects in both organizations.
- E. Create a third organization with a new host project, and attach all projects from your company and Altostrat to it using shared VPC.

Correct Answer: BC

Community vote distribution

BC (80%)

7%

7%

Question #15 Topic 1

Your on-premises data center has 2 routers connected to your Google Cloud environment through a VPN on each router. All applications are working correctly; however, all of the traffic is passing across a single VPN instead of being load-balanced across the 2 connections as desired.

During troubleshooting you find:

"⌘ Each on-premises router is configured with a unique ASN.

"⌘ Each on-premises router is configured with the same routes and priorities.

"⌘ Both on-premises routers are configured with a VPN connected to a single Cloud Router.

"⌘ BGP sessions are established between both on-premises routers and the Cloud Router.

"⌘ Only 1 of the on-premises router's routes are being added to the routing table.

What is the most likely cause of this problem?

- A. The on-premises routers are configured with the same routes.
- B. A firewall is blocking the traffic across the second VPN connection.
- C. You do not have a load balancer to load-balance the network traffic.
- D. The ASNs being used on the on-premises routers are different.

Correct Answer: D

Community vote distribution

D (100%)

Question #16 Topic 1

You have ordered Dedicated Interconnect in the GCP Console and need to give the Letter of Authorization/Connecting Facility Assignment (LOA-CFA) to your cross-connect provider to complete the physical connection.

Which two actions can accomplish this? (Choose two.)

- A. Open a Cloud Support ticket under the Cloud Interconnect category.
- B. Download the LOA-CFA from the Hybrid Connectivity section of the GCP Console.
- C. Run `gcloud compute interconnects describe <interconnect>`.
- D. Check the email for the account of the NOC contact that you specified during the ordering process.
- E. Contact your cross-connect provider and inform them that Google automatically sent the LOA/CFA to them via email, and to complete the connection.

Correct Answer: BD

Community vote distribution

BD (75%)

DE (25%)

Question #17 Topic 1

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: B

Community vote distribution

B (100%)

Question #18 Topic 1

Your company's web server administrator is migrating on-premises backend servers for an application to GCP. Libraries and configurations differ significantly across these backend servers. The migration to GCP will be lift-and-shift, and all requests to the servers will be served by a single network load balancer frontend.

You want to use a GCP-native solution when possible.

How should you deploy this service in GCP?

- A. Create a managed instance group from one of the images of the on-premises servers, and link this instance group to a target pool behind your load balancer.
- B. Create a target pool, add all backend instances to this target pool, and deploy the target pool behind your load balancer.
- C. Deploy a third-party virtual appliance as frontend to these servers that will accommodate the significant differences between these backend servers.
- D. Use GCP's ECMP capability to load-balance traffic to the backend servers by installing multiple equal-priority static routes to the backend servers.

Correct Answer: B

Community vote distribution

B (100%)

Question #19 Topic 1

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

Community vote distribution

B (100%)

Question #20 Topic 1

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

Correct Answer: D

Community vote distribution

D (80%)

B (20%)

Question #21 Topic 1

You are increasing your usage of Cloud VPN between on-premises and GCP, and you want to support more traffic than a single tunnel can handle. You want to increase the available bandwidth using Cloud VPN. What should you do?

- A. Double the MTU on your on-premises VPN gateway from 1460 bytes to 2920 bytes.
- B. Create two VPN tunnels on the same Cloud VPN gateway that point to the same destination VPN gateway IP address.
- C. Add a second on-premises VPN gateway with a different public IP address. Create a second tunnel on the existing Cloud VPN gateway that forwards the same IP range, but points at the new on-premises gateway IP.
- D. Add a second Cloud VPN gateway in a different region than the existing VPN gateway. Create a new tunnel on the second Cloud VPN gateway that forwards the same IP range, but points to the existing on-premises VPN gateway IP address.

Correct Answer: C

Community vote distribution



Question #22 Topic 1

You are disabling DNSSEC for one of your Cloud DNS-managed zones. You removed the DS records from your zone file, waited for them to expire from the cache, and disabled DNSSEC for the zone. You receive reports that DNSSEC validating resolves are unable to resolve names in your zone. What should you do?

- A. Update the TTL for the zone.
- B. Set the zone to the TRANSFER state.
- C. Disable DNSSEC at your domain registrar.
- D. Transfer ownership of the domain to a new registrar.

Correct Answer: C

Community vote distribution



Question #23 Topic 1

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.

Correct Answer: C

Community vote distribution



Question #24 Topic 1

You have configured Cloud CDN using HTTP(S) load balancing as the origin for cacheable content. Compression is configured on the web servers, but responses served by Cloud CDN are not compressed.

What is the most likely cause of the problem?

- A. You have not configured compression in Cloud CDN.
- B. You have configured the web servers and Cloud CDN with different compression types.
- C. The web servers behind the load balancer are configured with different compression types.
- D. You have to configure the web servers to compress responses even if the request has a Via header.

Correct Answer: D

Community vote distribution



Question #25 Topic 1

You have a web application that is currently hosted in the us-central1 region. Users experience high latency when traveling in Asia. You've configured a network load balancer, but users have not experienced a performance improvement. You want to decrease the latency.

What should you do?

- A. Configure a policy-based route rule to prioritize the traffic.
- B. Configure an HTTP load balancer, and direct the traffic to it.
- C. Configure Dynamic Routing for the subnet hosting the application.
- D. Configure the TTL for the DNS zone to decrease the time between updates.

Correct Answer: B

Community vote distribution



Question #26 Topic 1

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.

Correct Answer: AE

Community vote distribution



Question #27 Topic 1

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 them. Use firewall rules to filter access between the specific networks.
- B. Create 2 shared VPCs within the shared VPC Host Project, and create a Cloud VPN/Cloud Router between them. Use Flexible Route Advertisement (FRA) to filter access between the specific networks.
- C. Create 2 shared VPCs within the shared VPC Service Project, and create a Cloud VPN/Cloud Router between them. Use Flexible Route Advertisement (FRA) to filter access between the specific networks.
- D. Create 1 VPC within the shared VPC Host Project, and share individual subnets with the Service Projects to filter access between the specific networks.

Correct Answer: D

Community vote distribution



Question #28 Topic 1

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.

Correct Answer: C

Community vote distribution



Question #29 Topic 1

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.

Correct Answer: D

Community vote distribution



Question #30 Topic 1

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.

Correct Answer: BD

Community vote distribution



Question #31 Topic 1

You are using a 10-Gbps direct peering connection to Google together with the gsutil tool to upload files to Cloud Storage buckets from on-premises servers. The on-premises servers are 100 milliseconds away from the Google peering point. You notice that your uploads are not using the full 10-Gbps bandwidth available to you. You want to optimize the bandwidth utilization of the connection.

What should you do on your on-premises servers?

- A. Tune TCP parameters on the on-premises servers.
- B. Compress files using utilities like tar to reduce the size of data being sent.
- C. Remove the -m flag from the gsutil command to enable single-threaded transfers.
- D. Use the perfdiag parameter in your gsutil command to enable faster performance: gsutil perfdiag gs://[BUCKET NAME].

Correct Answer: A

Community vote distribution



Question #32 Topic 1

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.

Correct Answer: A

Community vote distribution



Question #33 Topic 1

You are designing a Google Kubernetes Engine (GKE) cluster for your organization. The current cluster size is expected to host 10 nodes, with 20 Pods per node and 150 services. Because of the migration of new services over the next 2 years, there is a planned growth for 100 nodes, 200 Pods per node, and 1500 services. You want to use VPC-native clusters with alias IP ranges, while minimizing address consumption.

How should you design this topology?

- A. Create a subnet of size/25 with 2 secondary ranges of: /17 for Pods and /21 for Services. Create a VPC-native cluster and specify those ranges.
- B. Create a subnet of size/28 with 2 secondary ranges of: /24 for Pods and /24 for Services. Create a VPC-native cluster and specify those ranges. When the services are ready to be deployed, resize the subnets.
- C. Use gcloud container clusters create [CLUSTER NAME]--enable-ip-alias to create a VPC-native cluster.
- D. Use gcloud container clusters create [CLUSTER NAME] to create a VPC-native cluster.

Correct Answer: A

Community vote distribution

A (100%)

Question #34 Topic 1

Your company has recently expanded their EMEA-based operations into APAC. Globally distributed users report that their SMTP and IMAP services are slow.

Your company requires end-to-end encryption, but you do not have access to the SSL certificates.

Which Google Cloud load balancer should you use?

- A. SSL proxy load balancer
- B. Network load balancer
- C. HTTPS load balancer
- D. TCP proxy load balancer

Correct Answer: D

Community vote distribution

D (71%)

A (29%)

Question #35 Topic 1

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

Correct Answer: AC

Community vote distribution

AC (85%)

Other

Question #36 Topic 1

You have a storage bucket that contains the following objects:

[1]
[1]
[1]
[1]

Cloud CDN is enabled on the storage bucket, and all four objects have been successfully cached. You want to remove the cached copies of all the objects with the prefix folder-a, using the minimum number of commands.

What should you do?

- A. Add an appropriate lifecycle rule on the storage bucket.
- B. Issue a cache invalidation command with pattern /folder-a/*.
- C. Make sure that all the objects with prefix folder-a are not shared publicly.
- D. Disable Cloud CDN on the storage bucket. Wait 90 seconds. Re-enable Cloud CDN on the storage bucket.

Correct Answer: B

Community vote distribution

B (100%)

Question #37 Topic 1

Your company is running out of network capacity to run a critical application in the on-premises data center. You want to migrate the application to GCP. You also want to ensure that the Security team does not lose their ability to monitor traffic to and from Compute Engine instances.

Which two products should you incorporate into the solution? (Choose two.)

- A. VPC flow logs
- B. Firewall logs
- C. Cloud Audit logs
- D. Stackdriver Trace
- E. Compute Engine instance system logs

Correct Answer: AB

Community vote distribution

AB (100%)

Question #38 Topic 1

You want to apply a new Cloud Armor policy to an application that is deployed in Google Kubernetes Engine (GKE). You want to find out which target to use for your Cloud Armor policy.

Which GKE resource should you use?

- A. GKE Node
- B. GKE Pod
- C. GKE Cluster
- D. GKE Ingress

Correct Answer: D

Community vote distribution

D (100%)

Question #39 Topic 1

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.

Correct Answer: A

Community vote distribution



Question #40 Topic 1

You create multiple Compute Engine virtual machine instances to be used at 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

Correct Answer: D

Community vote distribution



Question #41 Topic 1

You want to configure load balancing for an internet-facing, standard voice-over-IP (VOIP) application. Which type of load balancer should you use?

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

Correct Answer: B

Community vote distribution



Question #42 Topic 1

You want to configure a NAT to perform address translation between your on-premises network blocks and GCP. Which NAT solution should you use?

- A. Cloud NAT
- B. An instance with IP forwarding enabled
- C. An instance configured with iptables DNAT rules
- D. An instance configured with iptables SNAT rules

Correct Answer: A

Community vote distribution



Question #43 Topic 1

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.

Correct Answer: A

Community vote distribution



Question #44 Topic 1

In order to provide subnet level isolation, you want to force instance-A in one subnet to route through a security appliance, called instance-B, in another subnet.

What should you do?

- A. Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with no tag.
- B. Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with a tag applied to instance-A.
- C. Delete the system-generated subnet route and create a specific route to instance-B with a tag applied to instance-A.
- D. Move instance-B to another VPC and, using multi-NIC, connect instance-B's interface to instance-A's network. Configure the appropriate routes to force traffic through to instance-A.

Correct Answer: B

Community vote distribution



Question #45 Topic 1

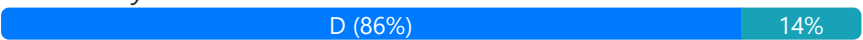
You create a Google Kubernetes Engine private cluster and want to use kubectl to get the status of the pods. In one of your instances you notice the master is not responding, even though the cluster is up and running.

What should you do to solve the problem?

- A. Assign a public IP address to the instance.
- B. Create a route to reach the Master, pointing to the default internet gateway.
- C. Create the appropriate firewall policy in the VPC to allow traffic from Master node IP address to the instance.
- D. Create the appropriate master authorized network entries to allow the instance to communicate to the master.

Correct Answer: D

Community vote distribution



Question #46 Topic 1

Your company has a security team that manages firewalls and SSL certificates. It also has a networking team that manages the networking resources. The networking team needs to be able to read firewall rules, but should not be able to create, modify, or delete them.

How should you set up permissions for the networking team?

- A. Assign members of the networking team the compute.networkUser role.
- B. Assign members of the networking team the compute.networkAdmin role.
- C. Assign members of the networking team a custom role with only the compute.networks.* and the compute.firewalls.list permissions.
- D. Assign members of the networking team the compute.networkViewer role, and add the compute.networks.use permission.

Correct Answer: B

Community vote distribution



Question #47 Topic 1

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.

Correct Answer: C

Community vote distribution



Question #48 Topic 1

You need to give each member of your network operations team least-privilege access to create, modify, and delete Cloud Interconnect VLAN attachments.

What should you do?

- A. Assign each user the editor role.
- B. Assign each user the compute.networkAdmin role.
- C. Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get.
- D. Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get, compute.routers.create, compute.routers.get, compute.routers.update.

Correct Answer: B

Community vote distribution



Question #49 Topic 1

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 group. Verify the new feature in the new canary instance group, and then update the original instance group.
- D. Perform a canary update by starting a rolling update and specifying a target size for your instances to receive the new template. Verify the new feature on the canary instances, and then roll forward to the rest of the instances.

Correct Answer: D

Community vote distribution



Question #50 Topic 1

You have deployed a proof-of-concept application by manually placing instances in a single Compute Engine zone. You are now moving the application to production, so you need to increase your application availability and ensure it can autoscale.

How should you provision your instances?

- A. Create a single managed instance group, specify the desired region, and select Multiple zones for the location.
- B. Create a managed instance group for each region, select Single zone for the location, and manually distribute instances across the zones in that region.
- C. Create an unmanaged instance group in a single zone, and then create an HTTP load balancer for the instance group.
- D. Create an unmanaged instance group for each zone, and manually distribute the instances across the desired zones.

Correct Answer: A

Community vote distribution



Question #51 Topic 1

You have a storage bucket that contains two objects. Cloud CDN is enabled on the bucket, and both objects have been successfully cached. Now you want to make sure that one of the two objects will not be cached anymore, and will always be served to the internet directly from the origin.

What should you do?

- A. Ensure that the object you don't want to be cached anymore is not shared publicly.
- B. Create a new storage bucket, and move the object you don't want to be checked anymore inside it. Then edit the bucket setting and enable the private attribute.
- C. Add an appropriate lifecycle rule on the storage bucket containing the two objects.
- D. Add a Cache-Control entry with value private to the metadata of the object you don't want to be cached anymore. Invalidate all the previously cached copies.

Correct Answer: D

Community vote distribution



Question #52 Topic 1

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.

Correct Answer: A

Community vote distribution



Question #53 Topic 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:

- ⇒ Your ISP is a Google Partner Interconnect provider.
- ⇒ Your on-premises VPN device's internet uplink and downlink speeds are 10 Gbps.
- ⇒ A test VPN connection between your on-premises gateway and GCP is performing at a maximum speed of 500 Mbps due to packet losses.
- ⇒ Most of the data transfer will be from GCP to the on-premises environment.
- ⇒ The application can burst up to 1.5 Gbps during peak transfers over the Interconnect.
- ⇒ 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: A

Community vote distribution



Question #54 Topic 1

Your company has just launched a new critical revenue-generating web application. You deployed the application for scalability using managed instance groups, autoscaling, and a network load balancer as frontend. One day, you notice severe bursty traffic that the caused autoscaling to reach the maximum number of instances, and users of your application cannot complete transactions. After an investigation, you think it as a DDOS attack. You want to quickly restore user access to your application and allow successful transactions while minimizing cost.

Which two steps should you take? (Choose two.)

- A. Use Cloud Armor to blacklist the attacker's IP addresses.
- B. Increase the maximum autoscaling backend to accommodate the severe bursty traffic.
- C. Create a global HTTP(s) load balancer and move your application backend to this load balancer.
- D. Shut down the entire application in GCP for a few hours. The attack will stop when the application is offline.
- E. SSH into the backend compute engine instances, and view the auth logs and syslogs to further understand the nature of the attack.

Correct Answer: AB

Community vote distribution

AB (55%)

AC (31%)

7%

Question #55 Topic 1

You are creating a new application and require access to Cloud SQL from VPC instances without public IP addresses. Which two actions should you take? (Choose two.)

- A. Activate the Service Networking API in your project.
- B. Activate the Cloud Datastore API in your project.
- C. Create a private connection to a service producer.
- D. Create a custom static route to allow the traffic to reach the Cloud SQL API.
- E. Enable Private Google Access.

Correct Answer: AC*Community vote distribution*

AC (67%)

AE (22%)

11%

Question #56 Topic 1

You want to use Cloud Interconnect to connect your on-premises network to a GCP VPC. You cannot meet Google at one of its point-of-presence (POP) locations, and your on-premises router cannot run a Border Gateway Protocol (BGP) configuration. Which connectivity model should you use?

- A. Direct Peering
- B. Dedicated Interconnect
- C. Partner Interconnect with a layer 2 partner
- D. Partner Interconnect with a layer 3 partner

Correct Answer: D*Community vote distribution*

D (76%)

C (24%)

Question #57 Topic 1

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`

Correct Answer: B*Community vote distribution*

B (100%)

Question #58 Topic 1

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

Correct Answer: C

Community vote distribution



Question #59 Topic 1

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.

Correct Answer: D

Community vote distribution



Question #60 Topic 1

Your company's Google Cloud-deployed, streaming application supports multiple languages. The application development team has asked you how they should support splitting audio and video traffic to different backend Google Cloud storage buckets. They want to use URL maps and minimize operational overhead. They are currently using the following directory structure:

```
/fr/video  
/en/video  
/es/video  
/./video  
/fr/audio  
/en/audio  
/es/audio  
/./audio
```

Which solution should you recommend?

- A. Rearrange the directory structure, create a URL map and leverage a path rule such as `/video/*` and `/audio/*`.
- B. Rearrange the directory structure, create DNS hostname entries for video and audio and leverage a path rule such as `/video/*` and `/audio/*`.
- C. Leave the directory structure as-is, create a URL map and leverage a path rule such as `\[a-z]{2}\video` and `\[a-z]{2}\audio`.
- D. Leave the directory structure as-is, create a URL map and leverage a path rule such as `/*video` and `/*audio`.

Correct Answer: A

Community vote distribution



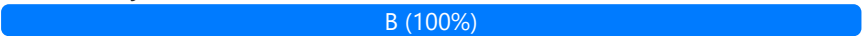
Question #61 Topic 1

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

Correct Answer: B

Community vote distribution



Question #62 Topic 1

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?

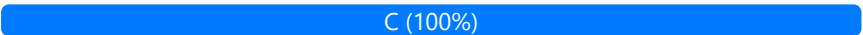
- A. VPC network in all projects
- B. VPC network in the IT Project
- C. VPC network in the Host Project
- D. VPC network in the Sales, Marketing, and IT Projects

Correct Answer: C

Reference:

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

Community vote distribution



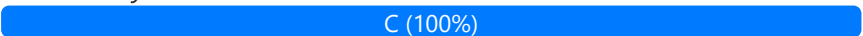
Question #63 Topic 1

You created a new VPC for your development team. You want to allow access to the resources in this VPC via SSH only.
How should you configure your firewall rules?

- A. Create two firewall rules: one to block all traffic with priority 0, and another to allow port 22 with priority 1000.
- B. Create two firewall rules: one to block all traffic with priority 65536, and another to allow port 3389 with priority 1000.
- C. Create a single firewall rule to allow port 22 with priority 1000.
- D. Create a single firewall rule to allow port 3389 with priority 1000.

Correct Answer: C

Community vote distribution



Question #64 Topic 1

Your on-premises data center has 2 routers connected to your GCP through a VPN on each router. All applications are working correctly; however, all of the traffic is passing across a single VPN instead of being load-balanced across the 2 connections as desired.

During troubleshooting you find:

"⌘ Each on-premises router is configured with the same ASN.

"⌘ Each on-premises router is configured with the same routes and priorities.

"⌘ Both on-premises routers are configured with a VPN connected to a single Cloud Router.

"⌘ The VPN logs have no-proposal-chosen lines when the VPNs are connecting.

"⌘ BGP session is not established between one on-premises router and the Cloud Router.

What is the most likely cause of this problem?

- A. One of the VPN sessions is configured incorrectly.
- B. A firewall is blocking the traffic across the second VPN connection.
- C. You do not have a load balancer to load-balance the network traffic.
- D. BGP sessions are not established between both on-premises routers and the Cloud Router.

Correct Answer: A

Community vote distribution



Question #65 Topic 1

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: B

Community vote distribution



Question #66 Topic 1

You have created a firewall with rules that only allow traffic over HTTP, HTTPS, and SSH ports. While testing, you specifically try to reach the server over multiple ports and protocols; however, you do not see any denied connections in the firewall logs. You want to resolve the issue.

What should you do?

- A. Enable logging on the default Deny Any Firewall Rule.
- B. Enable logging on the VM Instances that receive traffic.
- C. Create a logging sink forwarding all firewall logs with no filters.
- D. Create an explicit Deny Any rule and enable logging on the new rule.

Correct Answer: D

Community vote distribution



Question #67 Topic 1

In your company, two departments with separate GCP projects (code-dev and data-dev) in the same organization need to allow full cross-communication between all of their virtual machines in GCP. Each department has one VPC in its project and wants full control over their network. Neither department intends to recreate its existing computing resources. You want to implement a solution that minimizes cost.

Which two steps should you take? (Choose two.)

- A. Connect both projects using Cloud VPN.
- B. Connect the VPCs in project code-dev and data-dev using VPC Network Peering.
- C. Enable Shared VPC in one project (e. g., code-dev), and make the second project (e. g., data-dev) a service project.
- D. Enable firewall rules to allow all ingress traffic from all subnets of project code-dev to all instances in project data-dev, and vice versa.
- E. Create a route in the code-dev project to the destination prefixes in project data-dev and use nexthop as the default gateway, and vice versa.

Correct Answer: BD

Community vote distribution

BD (80%)

BE (20%)

Question #68 Topic 1

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.

Correct Answer: D

Community vote distribution

D (83%)

A (17%)

Question #69 Topic 1

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.

Correct Answer: AC

Community vote distribution

AC (100%)

Question #70 Topic 1

You are in the early stages of planning a migration to GCP. You want to test the functionality of your hybrid cloud design before you start to implement it in production. The design includes services running on a Compute Engine Virtual Machine instance that need to communicate to on-premises servers using private IP addresses. The on-premises servers have connectivity to the internet, but you have not yet established any Cloud Interconnect connections. You want to choose the lowest cost method of enabling connectivity between your instance and on-premises servers and complete the test in 24 hours.

Which connectivity method should you choose?

- A. Cloud VPN
- B. 50-Mbps Partner VLAN attachment
- C. Dedicated Interconnect with a single VLAN attachment
- D. Dedicated Interconnect, but don't provision any VLAN attachments

Correct Answer: A

Community vote distribution

A (100%)

Question #71 Topic 1

You want to implement an IPSec tunnel between your on-premises network and a VPC via Cloud VPN. You need to restrict reachability over the tunnel to specific local subnets, and you do not have a device capable of speaking Border Gateway Protocol (BGP).

Which routing option should you choose?

- A. Dynamic routing using Cloud Router
- B. Route-based routing using default traffic selectors
- C. Policy-based routing using a custom local traffic selector
- D. Policy-based routing using the default local traffic selector

Correct Answer: C

Community vote distribution

C (100%)

Question #72 Topic 1

You have enabled HTTP(S) load balancing for your application, and your application developers have reported that HTTP(S) requests are not being distributed correctly to your Compute Engine Virtual Machine instances. You want to find data about how the request are being distributed.

Which two methods can accomplish this? (Choose two.)

- A. On the Load Balancer details page of the GCP Console, click on the Monitoring tab, select your backend service, and look at the graphs.
- B. In Stackdriver Error Reporting, look for any unacknowledged errors for the Cloud Load Balancers service.
- C. In Stackdriver Monitoring, select Resources > Metrics Explorer and search for https/request_bytes_count metric.
- D. In Stackdriver Monitoring, select Resources > Google Cloud Load Balancers and review the Key Metrics graphs in the dashboard.
- E. In Stackdriver Monitoring, create a new dashboard and track the https/backend_request_count metric for the load balancer.

Correct Answer: AE

Community vote distribution

AE (100%)

Question #73 Topic 1

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`.

Correct Answer: C

Community vote distribution

C (80%)

B (20%)

Question #74 Topic 1

You need to centralize the Identity and Access Management permissions and email distribution for the WebServices Team as efficiently as possible.

What should you do?

- A. Create a Google Group for the WebServices Team.
- B. Create a G Suite Domain for the WebServices Team.
- C. Create a new Cloud Identity Domain for the WebServices Team.
- D. Create a new Custom Role for all members of the WebServices Team.

Correct Answer: A

Community vote distribution

A (100%)

Question #75 Topic 1

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.

Correct Answer: C

Reference:

<https://cloud.google.com/iam/docs/understanding-custom-roles>

Community vote distribution

C (100%)

Question #76 Topic 1

One instance in your VPC is configured to run with a private IP address only. You want to ensure that even if this instance is deleted, its current private IP address will not be automatically assigned to a different instance. In the GCP Console, what should you do?

- A. Assign a public IP address to the instance.
- B. Assign a new reserved internal IP address to the instance.
- C. Change the instance's current internal IP address to static.
- D. Add custom metadata to the instance with key internal-address and value reserved.

Correct Answer: C

Community vote distribution

C (100%)

Question #77 Topic 1

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.

Correct Answer: B

Community vote distribution

B (100%)

Question #78 Topic 1

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: C

Community vote distribution

C (100%)

Question #79 Topic 1

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

Correct Answer: D

Community vote distribution



Question #80 Topic 1

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.

Correct Answer: B

Community vote distribution



Question #81 Topic 1

Your company's security team tends to use managed services when possible. You need to build a dashboard to show the number of deny hits that occur against configured firewall rules without increasing operational overhead. What should you do?

- A. Configure Firewall Rules Logging. Use Firewall Insights to display the number of hits.
- B. Configure Firewall Rules Logging. View the logs in Cloud Logging, and create a custom dashboard in Cloud Monitoring to display the number of hits.
- C. Configure a firewall appliance from the Google Cloud Marketplace. Route all traffic through this appliance, and apply the firewall rules at this layer. Use the firewall appliance to display the number of hits.
- D. Configure Packet Mirroring on the VPC. Apply a filter with an IP address list of the Denied Firewall rules. Configure an intrusion detection system (IDS) appliance as the receiver to display the number of hits.

Correct Answer: B

Community vote distribution



Question #82 Topic 1

You are configuring your Google Cloud environment to connect to your on-premises network. Your configuration must be able to reach Cloud Storage APIs and your Google Kubernetes Engine nodes across your private Cloud Interconnect network. You have already configured a Cloud Router with your Interconnect VLAN attachments. You now need to set up the appropriate router advertisement configuration on the Cloud Router. What should you do?

- A. Configure the route advertisement to the default setting.
- B. On the on-premises router, configure a static route for the storage API virtual IP address which points to the Cloud Router's link-local IP address.
- C. Configure the route advertisement to the custom setting, and manually add prefix 199.36.153.8/30 to the list of advertisements. Leave all other options as their default settings.

- D. Configure the route advertisement to the custom setting, and manually add prefix 199.36.153.8/30 to the list of advertisements. Advertise all visible subnets to the Cloud Router.

Correct Answer: D

Community vote distribution

D (78%)

B (17%)

6%

Question #83 Topic 1

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: C

Community vote distribution

C (88%)

13%

Question #84 Topic 1

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 Logs. Create a sink in Cloud Logging to send filtered egress VPC Flow Logs to the IDS.
- C. Create an internal TCP/UDP load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.
- D. Create an internal HTTP(S) load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.

Correct Answer: C

Community vote distribution

C (70%)

B (30%)

Question #85 Topic 1

You are developing an HTTP API hosted on a Compute Engine virtual machine instance that must be invoked only by multiple clients within the same Virtual Private Cloud (VPC). You want clients to be able to get the IP address of the service. What should you do?

- A. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwarding rule. Clients should use this IP address to connect to the service.
- B. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url `https://[INSTANCE_NAME].[ZONE].c.[PROJECT_ID].internal/`.
- C. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwarding rule. Then, define an A record in Cloud DNS. Clients should use the name of the A record to connect to the service.
- D. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url `https://[API_NAME]/[API_VERSION]/`.

Correct Answer: B

Community vote distribution



Question #86 Topic 1

You recently deployed Cloud VPN to connect your on-premises data center to Google Cloud. You need to monitor the usage of this VPN and set up alerts in case traffic exceeds the maximum allowed. You need to be able to quickly decide whether to add extra links or move to a Dedicated Interconnect. What should you do?

- A. In the Network Intelligence Center, check for the number of packet drops on the VPN.
- B. In the Google Cloud Console, use Monitoring Query Language to create a custom alert for bandwidth utilization.
- C. In the Monitoring section of the Google Cloud Console, use the Dashboard section to select a default dashboard for VPN usage.
- D. In the VPN section of the Google Cloud Console, select the VPN under hybrid connectivity, and then select monitoring to display utilization on the dashboard.

Correct Answer: B

Community vote distribution



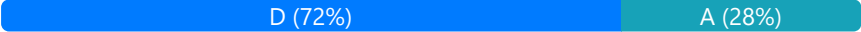
Question #87 Topic 1

You have applications running in the us-west1 and us-east1 regions. You want to build a highly available VPN that provides 99.99% availability to connect your applications from your project to the cloud services provided by your partner's project while minimizing the amount of infrastructure required. Your partner's services are also in the us-west1 and us-east1 regions. You want to implement the simplest solution. What should you do?

- A. Create one Cloud Router and one HA VPN gateway in each region of your VPC and your partner's VPC. Connect your VPN gateways to the partner's gateways. Enable global dynamic routing in each VPC.
- B. Create one Cloud Router and one HA VPN gateway in the us-west1 region of your VPC. Create one OpenVPN Access Server in each region of your partner's VPC. Connect your VPN gateway to your partner's servers.
- C. Create one OpenVPN Access Server in each region of your VPC and your partner's VPC. Connect your VPN gateway to your partner's servers.
- D. Create one Cloud Router and one HA VPN gateway in the us-west1 region of your VPC and your partner's VPC. Connect your VPN gateways to the partner's gateways with a pair of tunnels. Enable global dynamic routing in each VPC.

Correct Answer: D

Community vote distribution



Question #88 Topic 1

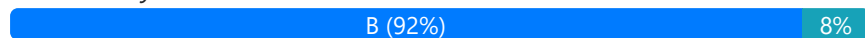
You need to create the network infrastructure to deploy a highly available web application in the us-east1 and us-west1 regions. The application runs on Compute Engine instances, and it does not require the use of a database. You want to follow Google-recommended practices. What should you do?

- A. Create one VPC with one subnet in each region.
Create a regional network load balancer in each region with a static IP address.
Enable Cloud CDN on the load balancers.
Create an A record in Cloud DNS with both IP addresses for the load balancers.
- B. Create one VPC with one subnet in each region.
Create a global load balancer with a static IP address.
Enable Cloud CDN and Google Cloud Armor on the load balancer.
Create an A record using the IP address of the load balancer in Cloud DNS.

- C. Create one VPC in each region, and peer both VPCs.
Create a global load balancer.
Enable Cloud CDN on the load balancer.
Create a CNAME for the load balancer in Cloud DNS.
- D. Create one VPC with one subnet in each region.
Create an HTTP(S) load balancer with a static IP address.
Choose the standard tier for the network.
Enable Cloud CDN on the load balancer.
Create a CNAME record using the load balancer's IP address in Cloud DNS.

Correct Answer: B

Community vote distribution



Question #89 Topic 1

You are the network administrator responsible for hybrid connectivity at your organization. Your developer team wants to use Cloud SQL in the us-west1 region in your Shared VPC. You configured a Dedicated Interconnect connection and a Cloud Router in us-west1, and the connectivity between your Shared VPC and on-premises data center is working as expected. You just created the private services access connection required for Cloud SQL using the reserved IP address range and default settings. However, your developers cannot access the Cloud SQL instance from on-premises. You want to resolve the issue. What should you do?

- A. 1. Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes.
2. Create a custom route advertisement in your Cloud Router to advertise the Cloud SQL IP address range.
- B. 1. Change the VPC routing mode to global.
2. Create a custom route advertisement in your Cloud Router to advertise the Cloud SQL IP address range.
- C. 1. Create an additional Cloud Router in us-west2.
2. Create a new Border Gateway Protocol (BGP) peering connection to your on-premises data center.
3. Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes.
- D. 1. Change the VPC routing mode to global.
2. Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes.

Correct Answer: A

Community vote distribution



Question #90 Topic 1

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 VPCs. Configure VPC Network Peering to export custom routes from Sales and import custom routes on Finance's VPC network. Use Cloud Router's custom route advertisements to announce a default route to the on-premises locations.
- D. Peer the two VPCs. Configure VPC Network Peering to export custom routes from Sales and import custom routes on Finance's VPC network. Use Cloud Router's custom route advertisements to announce the peered VPC network ranges to the on-premises locations.

Correct Answer: D

Community vote distribution



Question #91 Topic 1

You recently noticed a recurring daily spike in network usage in your Google Cloud project. You need to identify the virtual machine (VM) instances and type of traffic causing the spike in traffic utilization while minimizing the cost and management overhead required. What should you do?

- A. Enable VPC Flow Logs and send the output to BigQuery for analysis.
- B. Enable Firewall Rules Logging for all allowed traffic and send the output to BigQuery for analysis.
- C. Configure Packet Mirroring to send all traffic to a VM. Use Wireshark on the VM to identify traffic utilization for each VM in the VPC.
- D. Deploy a third-party network appliance and configure it as the default gateway. Use the third-party network appliance to identify users with high network traffic.

Correct Answer: A

Community vote distribution

A (94%)

6%

Question #92 Topic 1

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. 1. 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.
2. Create a custom route that points Google's restricted API address range to the default internet gateway as the next hop.
- B. 1. 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.
2. Change the custom route that points the default route (0/0) to the default internet gateway as the next hop.
- C. 1. 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.
2. Change the custom route that points the default route (0/0) to the default internet gateway as the next hop.
- D. 1. 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.
2. Create a custom route that points Google's private API address range to the default internet gateway as the next hop.

Correct Answer: A

Community vote distribution

A (60%)

B (30%)

10%

Question #93 Topic 1

You have deployed an HTTP(s) load balancer, but health checks to port 80 on the Compute Engine virtual machine instance are failing, and no traffic is sent to your instances. You want to resolve the problem. Which commands should you run?

- A. gcloud compute instances add-access-config instance-1
- B. gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --destination-ranges 130.211.0.0/22,35.191.0.0/16 --direction EGRESS
- C. gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --source-ranges 130.211.0.0/22,35.191.0.0/16 --direction INGRESS
- D. gcloud compute health-checks update http health-check --unhealthy-threshold 10

Correct Answer: C

Community vote distribution

C (100%)

Question #94 Topic 1

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.

Correct Answer: D

Community vote distribution

D (69%)

C (31%)

Question #95 Topic 1

You recently deployed your application in Google Cloud. You need to verify your Google Cloud network configuration before deploying your on-premises workloads. You want to confirm that your Google Cloud network configuration allows traffic to flow from your cloud resources to your on-premises network. This validation should also analyze and diagnose potential failure points in your Google Cloud network configurations without sending any data plane test traffic. What should you do?

- A. Use Network Intelligence Center's Connectivity Tests.
- B. Enable Packet Mirroring on your application and send test traffic.
- C. Use Network Intelligence Center's Network Topology visualizations.
- D. Enable VPC Flow Logs and send test traffic.

Correct Answer: C

Community vote distribution

C (75%)

A (25%)

Question #96 Topic 1

In your Google Cloud organization, you have two folders: Dev and Prod. You want a scalable and consistent way to enforce the following firewall rules for all virtual machines (VMs) with minimal cost:

- Port 8080 should always be open for VMs in the projects in the Dev folder.
- Any traffic to port 8080 should be denied for all VMs in your projects in the Prod folder.

What should you do?

- A. Create and associate a firewall policy with the Dev folder with a rule to open port 8080. Create and associate a firewall policy with the Prod folder with a rule to deny traffic to port 8080.
- B. Create a Shared VPC for the Dev projects and a Shared VPC for the Prod projects. Create a VPC firewall rule to open port 8080 in the Shared VPC for Dev. Create a firewall rule to deny traffic to port 8080 in the Shared VPC for Prod. Deploy VMs to those Shared VPCs.

- C. In all VPCs for the Dev projects, create a VPC firewall rule to open port 8080. In all VPCs for the Prod projects, create a VPC firewall rule to deny traffic to port 8080.
- D. Use Anthos Config Connector to enforce a security policy to open port 8080 on the Dev VMs and deny traffic to port 8080 on the Prod VMs.

Correct Answer: A

Community vote distribution



Question #97 Topic 1

You need to configure the Border Gateway Protocol (BGP) session for a VPN tunnel you just created between two Google Cloud VPCs, 10.1.0.0/16 and 172.16.0.0/16. You have a Cloud Router (router-1) in the 10.1.0.0/16 network and a second Cloud Router (router-2) in the 172.16.0.0/16 network. Which configuration should you use for the BGP session?

- A.

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	169.254.0.254	169.254.0.254	65502
router-2	if-tunnel-b-to-a-if-0	169.254.0.254	169.254.0.254	65501
- B.

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	10.1.0.1	172.16.0.1	15052
router-2	if-tunnel-b-to-a-if-0	172.16.0.1	10.1.0.1	15501
- C.

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	169.254.20.1	169.254.20.2	65002
router-2	if-tunnel-b-to-a-if-0	169.254.20.2	169.254.20.1	65001
- D.

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	172.16.0.254	10.1.0.254	16552
router-2	if-tunnel-b-to-a-if-0	10.1.0.254	172.16.0.254	16551

Correct Answer: C

Community vote distribution



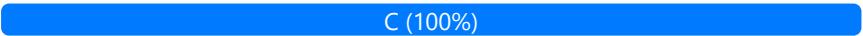
Question #98 Topic 1

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.

Correct Answer: C

Community vote distribution



Question #99 Topic 1

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.

Correct Answer: D

Community vote distribution

D (100%)

Question #100 Topic 1

You are designing the network architecture for your organization. Your organization has three developer teams: Web, App, and Database. All of the developer teams require access to Compute Engine instances to perform their critical tasks. You are part of a small network and security team that needs to provide network access to the developers. You need to maintain centralized control over network resources, including subnets, routes, and firewalls. You want to minimize operational overhead. How should you design this topology?

- A. Configure a host project with a Shared VPC. Create service projects for Web, App, and Database.
- B. Configure one VPC for Web, one VPC for App, and one VPC for Database. Configure HA VPN between each VPC.
- C. Configure three Shared VPC host projects, each with a service project: one for Web, one for App, and one for Database.
- D. Configure one VPC for Web, one VPC for App, and one VPC for Database. Use VPC Network Peering to connect all VPCs in a full mesh.

Correct Answer: A

Community vote distribution

A (100%)

Question #101 Topic 1

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 project. Create the relevant routes on the third-party appliances and VPC networks.
- B. Configure the third-party appliances with multiple interfaces, with each interface connected to a separate VPC network. Create separate VPC networks for on-premises and internet connectivity. Create the relevant routes on the third-party appliances and VPC networks.
- C. Consolidate all existing projects' subnetworks into a single VPC. Create separate VPC networks for on-premises and internet connectivity. Configure the third-party appliances with multiple interfaces, with each interface connected to a separate VPC

network. Create the relevant routes on the third-party appliances and VPC networks.

- D. Configure the third-party appliances with multiple interfaces. Create a hub VPC network for all projects, and create separate VPC networks for on-premises and internet connectivity. Create the relevant routes on the third-party appliances and VPC networks. Use VPC Network Peering to connect all projects' VPC networks to the hub VPC. Export custom routes from the hub VPC and import on all projects' VPC networks.

Correct Answer: D

Community vote distribution



Question #102 Topic 1

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

Correct Answer: B

Community vote distribution



Question #103 Topic 1

Your organization uses a hub-and-spoke architecture with critical Compute Engine instances in your Virtual Private Clouds (VPCs). You are responsible for the design of Cloud DNS in Google Cloud. You need to be able to resolve Cloud DNS private zones from your on-premises data center and enable on-premises name resolution from your hub-and-spoke VPC design. What should you do?

- A. 1. Configure a private DNS zone in the hub VPC, and configure DNS forwarding to the on-premises server.
2. Configure DNS peering from the spoke VPCs to the hub VPC.
- B. 1. Configure a DNS policy in the hub VPC to allow inbound query forwarding from the spoke VPCs.
2. Configure the spoke VPCs with a private zone, and set up DNS peering to the hub VPC.
- C. 1. Configure a DNS policy in the spoke VPCs, and configure your on-premises DNS as an alternate DNS server.
2. Configure the hub VPC with a private zone, and set up DNS peering to each of the spoke VPCs.
- D. 1. Configure a DNS policy in the hub VPC, and configure the on-premises DNS as an alternate DNS server.
2. Configure the spoke VPCs with a private zone, and set up DNS peering to the hub VPC.

Correct Answer: A

Community vote distribution



Question #104 Topic 1

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.

Correct Answer: B

Community vote distribution

B (100%)

Question #105 Topic 1

You are maintaining a Shared VPC in a host project. Several departments within your company have infrastructure in different service projects attached to the Shared VPC and use Identity and Access Management (IAM) permissions to manage the cloud resources in those projects. VPC Network Peering is also set up between the Shared VPC and a common services VPC that is not in a service project. Several users are experiencing failed connectivity between certain instances in different Shared VPC service projects and between certain instances and the internet. You need to validate the network configuration to identify whether a misconfiguration is the root cause of the problem. What should you do?

- A. Review the VPC audit logs in Cloud Logging for the affected instances.
- B. Use Secure Shell (SSH) to connect to the affected Compute Engine instances, and run a series of PING tests to the other affected endpoints and the 8.8.8.8 IPv4 address.
- C. Run Connectivity Tests from Network Intelligence Center to check connectivity between the affected endpoints in your network and the internet.
- D. Enable VPC Flow Logs for all VPCs, and review the logs in Cloud Logging for the affected instances.

Correct Answer: C

Community vote distribution

C (100%)

Question #106 Topic 1

Your organization has Compute Engine instances in us-east1, us-west2, and us-central1. Your organization also has an existing Cloud Interconnect physical connection in the East Coast of the United States with a single VLAN attachment and Cloud Router in us-east1. You need to provide a design with high availability and ensure that if a region goes down, you still have access to all your other Virtual Private Cloud (VPC) subnets. You need to accomplish this in the most cost-effective manner possible. What should you do?

- A. 1. Configure your VPC routing in regional mode.
2. Add an additional Cloud Interconnect VLAN attachment in the us-east1 region, and configure a Cloud Router in us-east1.
- B. 1. Configure your VPC routing in global mode.
2. Add an additional Cloud Interconnect VLAN attachment in the us-east1 region, and configure a Cloud Router in us-east1.
- C. 1. Configure your VPC routing in global mode.
2. Add an additional Cloud Interconnect VLAN attachment in the us-west2 region, and configure a Cloud Router in us-west2.
- D. 1. Configure your VPC routing in regional mode.
2. Add additional Cloud Interconnect VLAN attachments in the us-west2 and us-central1 regions, and configure Cloud Routers in us-west2 and us-central1.

Correct Answer: C

Community vote distribution



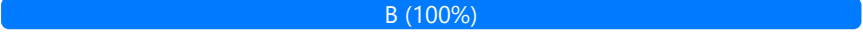
Question #107 Topic 1

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 identify 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 Cloud Console.

Correct Answer: B

Community vote distribution



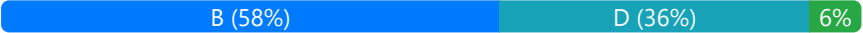
Question #108 Topic 1

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.

Correct Answer: B

Community vote distribution



Question #109 Topic 1

You recently deployed Compute Engine instances in regions us-west1 and us-east1 in a Virtual Private Cloud (VPC) with default routing configurations. Your company security policy mandates that virtual machines (VMs) must not have public IP addresses attached to them. You need to allow your instances to fetch updates from the internet while preventing external access. What should you do?

- A. Create a Cloud NAT gateway and Cloud Router in both us-west1 and us-east1.
- B. Create a single global Cloud NAT gateway and global Cloud Router in the VPC.
- C. Change the instances' network interface external IP address from None to Ephemeral.
- D. Create a firewall rule that allows egress to destination 0.0.0.0/0.

Correct Answer: A

Community vote distribution



Question #110 Topic 1

You are designing a new global application using Compute Engine instances that will be exposed by a global HTTP(S) load balancer. You need to secure your application from distributed denial-of-service and application layer (layer 7) attacks. What should you do?

- A. Configure VPC Service Controls and create a secure perimeter. Define fine-grained perimeter controls and enforce that security posture across your Google Cloud services and projects.
- B. Configure a Google Cloud Armor security policy in your project, and attach it to the backend service to secure the application.
- C. Configure VPC firewall rules to protect the Compute Engine instances against distributed denial-of-service attacks.
- D. Configure hierarchical firewall rules for the global HTTP(S) load balancer public IP address at the organization level.

Correct Answer: B

Community vote distribution

B (100%)

Question #111 Topic 1

Your organization's security policy requires that all internet-bound traffic return to your on-premises data center through HA VPN tunnels before egressing to the internet, while allowing virtual machines (VMs) to leverage private Google APIs using private virtual IP addresses 199.36.153.4/30. You need to configure the routes to enable these traffic flows. What should you do?

- A. Configure a custom route 0.0.0.0/0 with a priority of 500 whose next hop is the default internet gateway. Configure another custom route 199.36.153.4/30 with priority of 1000 whose next hop is the VPN tunnel back to the on-premises data center.
- B. Configure a custom route 0.0.0.0/0 with a priority of 1000 whose next hop is the internet gateway. Configure another custom route 199.36.153.4/30 with a priority of 500 whose next hop is the VPN tunnel back to the on-premises data center.
- C. Announce a 0.0.0.0/0 route from your on-premises router with a MED of 1000. Configure a custom route 199.36.153.4/30 with a priority of 1000 whose next hop is the default internet gateway.
- D. Announce a 0.0.0.0/0 route from your on-premises router with a MED of 500. Configure another custom route 199.36.153.4/30 with a priority of 1000 whose next hop is the VPN tunnel back to the on-premises data center.

Correct Answer: C

Community vote distribution

C (85%)

D (15%)

Question #112 Topic 1

Your company has defined a resource hierarchy that includes a parent folder with subfolders for each department. Each department defines their respective project and VPC in the assigned folder and has the appropriate permissions to create Google Cloud firewall rules. The VPCs should not allow traffic to flow between them. You need to block all traffic from any source, including other VPCs, and delegate only the intra-VPC firewall rules to the respective departments. What should you do?

- A. Create a VPC firewall rule in each VPC to block traffic from any source, with priority 0.
- B. Create a VPC firewall rule in each VPC to block traffic from any source, with priority 1000.
- C. Create two hierarchical firewall policies per department's folder with two rules in each: a high-priority rule that matches traffic from the private CIDRs assigned to the respective VPC and sets the action to allow, and another lower-priority rule that blocks traffic from any other source.
- D. Create two hierarchical firewall policies per department's folder with two rules in each: a high-priority rule that matches traffic from the private CIDRs assigned to the respective VPC and sets the action to goto_next, and another lower-priority rule that blocks traffic from any other source.

Correct Answer: D

Community vote distribution

D (64%)

C (36%)

Question #113 Topic 1

You have two Google Cloud projects in a perimeter to prevent data exfiltration. You need to move a third project inside the perimeter; however, the move could negatively impact the existing environment. You need to validate the impact of the change. What should you do?

- A. Enable Firewall Rules Logging inside the third project.
- B. Modify the existing VPC Service Controls policy to include the new project in dry run mode.
- C. Monitor the Resource Manager audit logs inside the perimeter.
- D. Enable VPC Flow Logs inside the third project, and monitor the logs for negative impact.

Correct Answer: B

Community vote distribution

B (100%)

Question #114 Topic 1

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.

Correct Answer: B

Community vote distribution

B (100%)

Question #115 Topic 1

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.

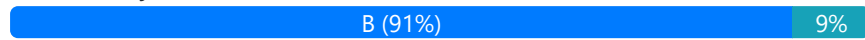
What should you do?

- A. 1. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range.
2. Create a CNAME record for *.googleapis.com that points to the A record.
3. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.
4. Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.
- B. 1. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range.
2. Create a CNAME record for *.googleapis.com that points to the A record.
3. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.
4. Configure your on-premises firewalls to allow traffic to the restricted.googleapis.com addresses.

- C. 1. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range.
2. Create a CNAME record for *.googleapis.com that points to the A record.
3. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.
4. Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.
- D. 1. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range.
2. Create a CNAME record for *.googleapis.com that points to the A record.
3. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.
4. Configure your on-premises firewalls to allow traffic to the private.googleapis.com addresses.

Correct Answer: B

Community vote distribution



Question #116 Topic 1

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 addresses. Configure a /25 secondary IP range for the Pods. Configure a /22 secondary IP range for the Services.
- B. Configure a /28 primary IP address range for the node IP addresses. Configure a /25 secondary IP range for the Pods. Configure a /21 secondary IP range for the Services.
- C. Configure a /28 primary IP address range for the node IP addresses. Configure a /28 secondary IP range for the Pods. Configure a /21 secondary IP range for the Services.
- D. Configure a /28 primary IP address range for the node IP addresses. Configure a /24 secondary IP range for the Pods. Configure a /22 secondary IP range for the Services.

Correct Answer: D

Community vote distribution



Question #117 Topic 1

You are migrating a three-tier application architecture from on-premises to Google Cloud. As a first step in the migration, you want to create a new Virtual Private Cloud (VPC) with an external HTTP(S) load balancer. This load balancer will forward traffic back to the on-premises compute resources that run the presentation tier. You need to stop malicious traffic from entering your VPC and consuming resources at the edge, so you must configure this policy to filter IP addresses and stop cross-site scripting (XSS) attacks. What should you do?

- A. Create a Google Cloud Armor policy, and apply it to a backend service that uses an unmanaged instance group backend.
- B. Create a hierarchical firewall ruleset, and apply it to the VPC's parent organization resource node.
- C. Create a Google Cloud Armor policy, and apply it to a backend service that uses an internet network endpoint group (NEG) backend.
- D. Create a VPC firewall ruleset, and apply it to all instances in unmanaged instance groups.

Correct Answer: C

Community vote distribution



Question #118 Topic 1

You just finished your company's migration to Google Cloud and configured an architecture with 3 Virtual Private Cloud (VPC) networks: one for Sales, one for Finance, and one for Engineering. Every VPC contains over 100 Compute Engine instances, and now developers using instances in the Sales VPC and the Finance VPC require private connectivity between each other. You need to allow communication between Sales and Finance without compromising performance or security. What should you do?

- A. Configure an HA VPN gateway between the Finance VPC and the Sales VPC.
- B. Configure the instances that require communication between each other with an external IP address.
- C. Create a VPC Network Peering connection between the Finance VPC and the Sales VPC.
- D. Configure Cloud NAT and a Cloud Router in the Sales and Finance VPCs.

Correct Answer: C

Community vote distribution

C (100%)

Question #119 Topic 1

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.

Correct Answer: D

Community vote distribution

D (100%)

Question #120 Topic 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.

Correct Answer: D

Community vote distribution

D (59%)

B (41%)

Question #121 Topic 1

In your project my-project, you have two subnets in a Virtual Private Cloud (VPC): subnet-a with IP range 10.128.0.0/20 and subnet-b with IP range 172.16.0.0/24. You need to deploy database servers in subnet-a. You will also deploy the application servers and web servers in subnet-b. You want to configure firewall rules that only allow database traffic from the application servers to the database servers. What should you do?

- A. Create network tag app-server and service account sa-db@my-project.iam.gserviceaccount.com. Add the tag to the application servers, and associate the service account with the database servers. Run the following command: gcloud compute firewall-rules create app-db-firewall-rule \

--action allow \

--direction ingress \

--rules top:3306 \

--source-tags app-server \

--target-service-accounts sa-db@my-project.iam.gserviceaccount.com
- B. Create service accounts sa-app@my-project.iam.gserviceaccount.com and sa-db@my-project.iam.gserviceaccount.com. Associate service account sa-app with the application servers, and associate the service account sa-db with the database servers. Run the following command: gcloud compute firewall-rules create app-db-firewall-ru

--allow TCP:3306 \

--source-service-accounts sa-app@democloud-idp-demo.iam.gserviceaccount.com \

--target-service-accounts sa-db@my-project.iam.gserviceaccount.com
- C. Create service accounts sa-app@my-project.iam.gserviceaccount.com and sa-db@my-project.iam.gserviceaccount.com. Associate the service account sa-app with the application servers, and associate the service account sa-db with the database servers. Run the following command: gcloud compute firewall-rules create app-db-firewall-ru

--allow TCP:3306 \

--source-ranges 10.128.0.0/20 \

--source-service-accounts sa-app@my-project.iam.gserviceaccount.com \

--target-service-accounts sa-db@my-project.iam.gserviceaccount.com
- D. Create network tags app-server and db-server. Add the app-server tag to the application servers, and add the db-server tag to the database servers. Run the following command: gcloud compute firewall-rules create app-db-firewall-rule \

--action allow \

--direction ingress \

--rules tcp:3306 \

--source-ranges 10.128.0.0/20 \

--source-tags app-server \

--target-tags db-server

Correct Answer: B

Community vote distribution

B (87%)

7%

Question #122 Topic 1

You are planning a large application deployment in Google Cloud that includes on-premises connectivity. The application requires direct connectivity between workloads in all regions and on-premises locations without address translation, but all RFC 1918 ranges are already in use in the on-premises locations. What should you do?

- A. Use multiple VPC networks with a transit network using VPC Network Peering.
- B. Use overlapping RFC 1918 ranges with multiple isolated VPC networks.
- C. Use overlapping RFC 1918 ranges with multiple isolated VPC networks and Cloud NAT.
- D. Use non-RFC 1918 ranges with a single global VPC.

Correct Answer: D

Community vote distribution

D (100%)

Question #123 Topic 1

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 80 and 443.

Correct Answer: C

Community vote distribution

C (100%)

Question #124 Topic 1

You successfully provisioned a single Dedicated Interconnect. The physical connection is at a colocation facility closest to us-west2. Seventy-five percent of your workloads are in us-east4, and the remaining twenty-five percent of your workloads are in us-central1. All workloads have the same network traffic profile. You need to minimize data transfer costs when deploying VLAN attachments. What should you do?

- A. Keep the existing Dedicated interconnect. Deploy a VLAN attachment to a Cloud Router in us-west2, and use VPC global routing to access workloads in us-east4 and us-central1.
- B. Keep the existing Dedicated Interconnect. Deploy a VLAN attachment to a Cloud Router in us-east4, and deploy another VLAN attachment to a Cloud Router in us-central1.
- C. Order a new Dedicated Interconnect for a colocation facility closest to us-east4, and use VPC global routing to access workloads in us-central1.
- D. Order a new Dedicated Interconnect for a colocation facility closest to us-central1, and use VPC global routing to access workloads in us-east4.

Correct Answer: B

Community vote distribution

B (79%)

C (21%)

Question #125 Topic 1

You are designing a hybrid cloud environment. Your Google Cloud environment is interconnected with your on-premises network using HA VPN and Cloud Router in a central transit hub VPC. The Cloud Router is configured with the default settings. Your on-premises DNS server is located at 192.168.20.88. You need to ensure that your Compute Engine resources in multiple spoke VPCs can resolve on-premises private hostnames using the domain corp.altostrat.com while also resolving Google Cloud hostnames. You want to follow Google-recommended practices. What should you do?

- A. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88. Associate the zone with the hub VPC.
2. Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.
3. Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
4. Configure VPC peering in the spoke VPCs to peer with the hub VPC.
- B. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
2. Associate the zone with the hub VPC. Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke PCs, with the hub VPC as the target.
3. Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
- C. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88. Associate the zone with the hub VPC.

2. Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.
 3. Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
 4. Create a hub-and-spoke VPN deployment in each spoke VPC to connect back to the on-premises network directly.
- D. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88. Associate the zone with the hub VPC.
 - 2. Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.
 - 3. Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
 - 4. Create a hub and spoke VPN deployment in each spoke VPC to connect back to the hub VPC.

Correct Answer: A

Community vote distribution



Question #126 Topic 1

You have the following firewall ruleset applied to all instances in your Virtual Private Cloud (VPC):

Direction	Action	Address range	Port	Priority
egress	deny	192.0.2.0/24	80	100
egress	deny	198.51.100.0/24	80	200
ingress	allow	203.0.113.0/24	80	300

You need to update the firewall rule to add the following rule to the ruleset:

Direction	Action	Address range	Port	Logging
egress	deny	192.0.2.42/32	80	true

You are using a new user account. You must assign the appropriate identity and Access Management (IAM) user roles to this new user account before updating the firewall rule. The new user account must be able to apply the update and view firewall logs. What should you do?

- A. Assign the compute.securityAdmin and logging.viewer rule to the new user account. Apply the new firewall rule with a priority of 50.
- B. Assign the compute.securityAdmin and logging.bucketWriter role to the new user account. Apply the new firewall rule with a priority of 150.
- C. Assign the compute.orgSecurityPolicyAdmin and logging.viewer role to the new user account. Apply the new firewall rule with a priority of 50.
- D. Assign the compute.orgSecurityPolicyAdmin and logging.bucketWriter role to the new user account. Apply the new firewall rule with a priority of 150.

Correct Answer: A

Community vote distribution



Question #127 Topic 1

Your organization has a single project that contains multiple Virtual Private Clouds (VPCs). You need to secure API access to your Cloud Storage buckets and BigQuery datasets by allowing API access only from resources in your corporate public networks. What should you do?

- A. Create an access context policy that allows your VPC and corporate public network IP ranges, and then attach the policy to Cloud Storage and BigQuery.
- B. Create a VPC Service Controls perimeter for your project with an access context policy that allows your corporate public network IP ranges.
- C. Create a firewall rule to block API access to Cloud Storage and BigQuery from unauthorized networks.

- D. Create a VPC Service Controls perimeter for each VPC with an access context policy that allows your corporate public network IP ranges.

Correct Answer: B

Community vote distribution

B (100%)

Question #128 Topic 1

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.

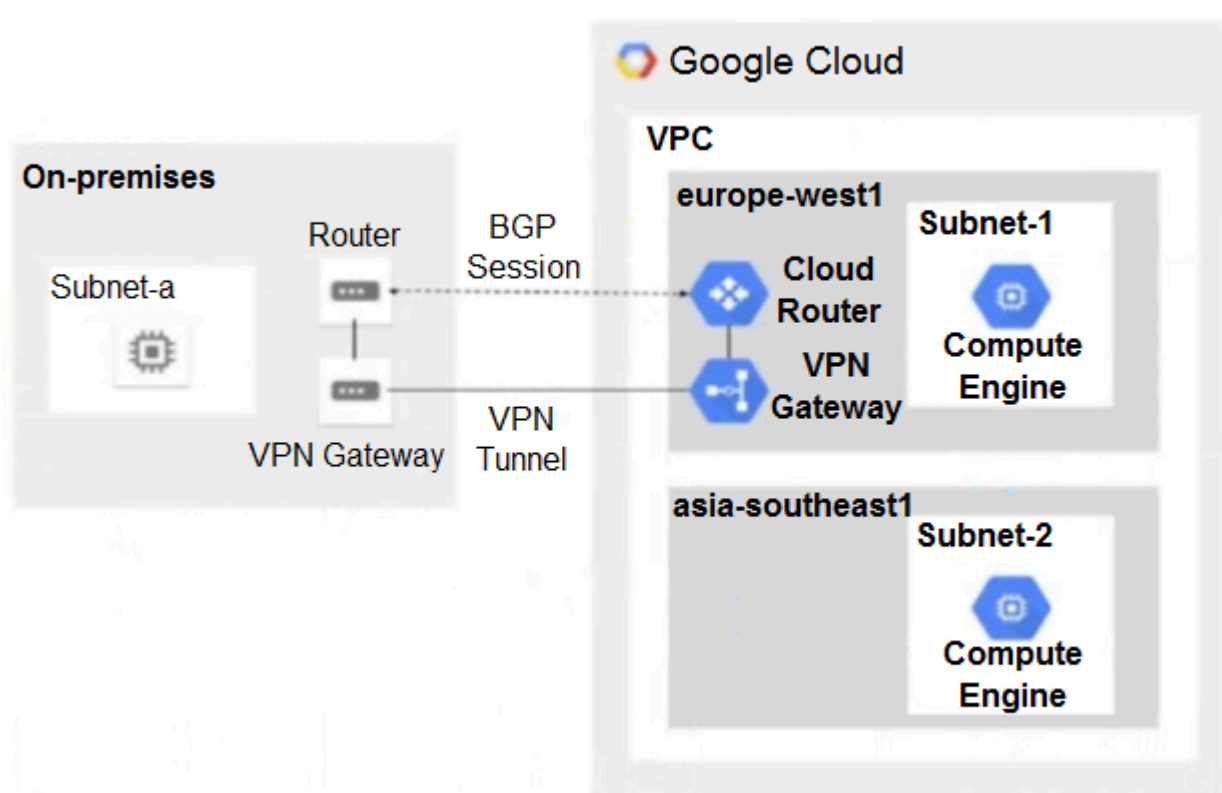
Correct Answer: DE

Community vote distribution

DE (100%)

Question #129 Topic 1

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?



- 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.

Correct Answer: C

Community vote distribution

C (100%)

Question #130 Topic 1

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. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
2. Configure your on-premises firewall to accept traffic from 10.204.0.0/24.
3. Set a custom route advertisement on the Cloud Router for 10.204.0.0/24
- B. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
2. Configure your on-premises firewall to accept traffic from 35.199.192.0/19
3. Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
- C. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
2. Configure your on-premises firewall to accept traffic from 10.204.0.0/24.
3. Modify the /etc/resolv.conf file on your Compute Engine instances to point to 192.168.20.88
- D. 1. Create a private zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com.
2. Configure DNS Server Policies and create a policy with Alternate DNS servers to 192.168.20.88.
3. Configure your on-premises firewall to accept traffic from 35.199.192.0/19.
4. Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.

Correct Answer: B

Community vote distribution

B (100%)

Question #131 Topic 1

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?

- 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.

Correct Answer: A

Community vote distribution

A (88%)

13%

Question #132 Topic 1

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?

- 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.

Correct Answer: B

Community vote distribution

B (100%)

Question #133 Topic 1

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.

Correct Answer: D

Community vote distribution

D (100%)

Question #134 Topic 1

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?

- 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.

Correct Answer: D

Community vote distribution

D (69%)

C (31%)

Question #135 Topic 1

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?

- A. 1. Delete the default route in your VPC.
2. 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.
3. 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. 1. 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).
2. 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.
3. 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. 1. 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.
2. Create a private Cloud DNS zone for 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.
3. 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. 1. 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).
2. Create a private Cloud DNS zone for 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.
3. Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.

Correct Answer: D

Community vote distribution



Question #136 Topic 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?

- A. 1. Create a default route in the hub VPC that points to IP address 10.0.0.5.
2. 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.
3. Export the custom routes in the hub.
4. Import the custom routes in the spokes.
- B. 1. Create a default route in the hub VPC that points to IP address 10.0.0.5.
2. 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.
3. Export the custom routes in the hub. Import the custom routes in the spokes.
4. Delete the default internet gateway route of the spokes.
- C. 1. Create two default routes in the hub VPC that point to the next hop instances of the virtual appliances.
2. 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.
3. Export the custom routes in the hub. Import the custom routes in the spokes.
- D. 1. Create a default route in the hub VPC that points to IP address 10.0.0.5.
2. 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.
3. Create a new route in the spoke VPC that points to IP address 10.0.0.5.

Correct Answer: B

Community vote distribution

B (78%)

A (22%)

Question #137 Topic 1

You configured Cloud VPN with dynamic routing via Border Gateway Protocol (BGP). You added a custom route to advertise a network that is reachable over the VPN tunnel. However, the on-premises clients still cannot reach the network over the VPN tunnel. You need to examine the logs in Cloud Logging to confirm that the appropriate routers are being advertised over the VPN tunnel. Which filter should you use in Cloud Logging to examine the logs?

- A. resource.type= "gce_router"
- B. resource.type= "gce_network_region"
- C. resource.type= "vpn_tunnel"
- D. resource.type= "vpn_gateway"

Correct Answer: A

Community vote distribution

A (73%)

D (20%)

7%

Question #138 Topic 1

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.

Correct Answer: B

Community vote distribution

B (75%)

C (25%)

Question #139 Topic 1

Your organization has a Google Cloud Virtual Private Cloud (VPC) with subnets in us-east1, us-west4, and europe-west4 that use the default VPC configuration. Employees in a branch office in Europe need to access the resources in the VPC using HA VPN. You configured the HA VPN associated with the Google Cloud VPC for your organization with a Cloud Router deployed in europe-west4. You need to ensure that the users in the branch office can quickly and easily access all resources in the VPC. What should you do?

- A. Create custom advertised routes for each subnet.
- B. Configure each subnet's VPN connections to use Cloud VPN to connect to the branch office.
- C. Configure the VPC dynamic routing mode to Global.
- D. Set the advertised routes to Global for the Cloud Router.

Correct Answer: C

Community vote distribution

C (100%)

Question #140 Topic 1

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. 1. 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.
2. In your Cloud Router, add a custom route advertisement for the IP 35.199.192.0/19 to the on-premises environment.
- B. 1. 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.
2. In your Cloud Router, add a custom route advertisement for the IP 169.254 169.254 to the on-premises environment.
- C. 1. Configure a Cloud DNS private zone in the host project of the Shared VPC.
2. 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
3. In your Cloud Router, add a custom route advertisement for the IP 169.254 169 254 to the on-premises environment.
- D. 1. Configure a Cloud DNS private zone in the host project of the Shared VPC.
2. 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.
3. Configure a DNS policy in the Shared VPC to allow inbound query forwarding with your on-premises DNS server as the alternative DNS server.

Correct Answer: A

Community vote distribution

A (100%)

Question #141 Topic 1

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: allow -

Target: VM B service account -

Source ranges: VM A service account

Priority: 1000

- B. Firewall rule direction: ingress

Action: allow -

Target: specific VM B tag -

Source ranges: VM A tag and VM A source IP address

Priority: 1000

- C. Firewall rule direction: ingress

Action: allow -

Target: VM A service account -

Source ranges: VM B service account and VM B source IP address

Priority: 100

- D. Firewall rule direction: ingress

Action: allow -

Target: specific VM A tag -

Source ranges: VM B tag and VM B source IP address

Priority: 100

Correct Answer: A

Community vote distribution



Question #142 Topic 1

You have configured a service on Google Cloud that connects to an on-premises service via a Dedicated Interconnect. Users are reporting recent connectivity issues. You need to determine whether the traffic is being dropped because of firewall rules or a routing decision. What should you do?

- A. Use the Network Intelligence Center Connectivity Tests to test the connectivity between the VPC and the on-premises network.
- B. Use Network Intelligence Center Network Topology to check the traffic flow, and replay the traffic from the time period when the connectivity issue occurred.
- C. Configure VPC Flow Logs. Review the logs by filtering on the source and destination.
- D. Configure a Compute Engine instance on the same VPC as the service running on Google Cloud to run a traceroute targeted at the on-premises service.

Correct Answer: A

Community vote distribution



Question #143 Topic 1

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

Correct Answer: D

Community vote distribution



Question #144 Topic 1

Your team is developing an application that will be used by consumers all over the world. Currently, the application sits behind a global external application load balancer. You need to protect the application from potential application-level attacks. What should you do?

- A. Enable Cloud CDN on the backend service.
- B. Create multiple firewall deny rules to block malicious users, and apply them to the global external application load balancer.

- C. Create a Google Cloud Armor security policy with web application firewall rules, and apply the security policy to the backend service
- D. Create a VPC Service Controls perimeter with the global external application load balancer as the protected service, and apply it to the backend service.

Correct Answer: C

Community vote distribution

C (100%)

Question #145 Topic 1

You are responsible for designing a new connectivity solution for your organization's enterprise network to access and use Google Workspace. You have an existing Shared VPC with Compute Engine instances in us-west1. Currently, you access Google Workspace via your service provider's internet access. You want to set up a direct connection between your network and Google. What should you do?

- A. Order a Dedicated Interconnect connection in the same metropolitan area. Create a VLAN attachment, a Cloud Router in us-west1, and a Border Gateway Protocol (BGP) session between your Cloud Router and your router.
- B. Order a Direct Peering connection in the same metropolitan area. Configure a Border Gateway Protocol (BGP) session between Google and your router.
- C. Configure HA VPN in us-west1. Configure a Border Gateway Protocol (BGP) session between your Cloud Router and your on-premises data center.
- D. Order a Carrier Peering connection in the same metropolitan area. Configure a Border Gateway Protocol (BGP) session between Google and your router.

Correct Answer: B

Community vote distribution

B (83%)

D (17%)

Question #146 Topic 1

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 VPC. Analyze the logs and get the source IP addresses from the subnetworks.get field.
- B. Enable VPC Flow Logs for the subnet. Analyze the logs and get the source IP addresses from the connection field.
- C. Enable VPC Flow Logs for the VPC. Analyze the logs and get the source IP addresses from the src_location field.
- D. Enable Data Access audit logs of the subnet. Analyze the logs and get the source IP addresses from the networks.get field.

Correct Answer: B

Community vote distribution

B (75%)

C (25%)

Question #147 Topic 1

You are responsible for configuring firewall policies for your company in Google Cloud. Your security team has a strict set of requirements that must be met to configure firewall rules.

- Always allow Secure Shell (SSH) from your corporate IP address.
- Restrict SSH access from all other IP addresses.

There are multiple projects and VPCs in your Google Cloud organization. You need to ensure that other VPC firewall rules cannot bypass the security team's requirements. What should you do?

- A. 1. Configure a hierarchical firewall policy to the organization node to allow TCP port 22 for your corporate IP address with priority 0.
2. Configure a hierarchical firewall policy to the organization node to deny TCP port 22 for all IP addresses with priority 1.
- B. 1. Configure a VPC firewall rule to allow TCP port 22 for your corporate IP address with priority 0.
2. Configure a VPC firewall rule to deny TCP port 22 for all IP addresses with priority 1.
- C. 1. Configure a VPC firewall rule to allow TCP port 22 for your corporate IP address with priority 1.
2. Configure a VPC firewall rule to deny TCP port 22 for all IP addresses with priority 0.
- D. 1. Configure a hierarchical firewall policy to the organization node to allow TCP port 22 for your corporate IP address with priority 1
2. Configure a hierarchical firewall policy to the organization node to deny TCP port 22 for all IP addresses with priority 0.

Correct Answer: A

Community vote distribution



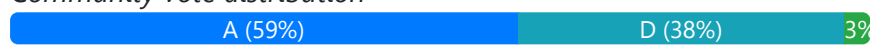
Question #148 Topic 1

You are designing a new application that has backends internally exposed on port 800. The application will be exposed externally using both IPv4 and IPv6 via TCP on port 700. You want to ensure high availability for this application. What should you do?

- A. Create a network load balancer that used backend services containing one instance group with two instances.
- B. Create a network load balancer that uses a target pool backend with two instances.
- C. Create a TCP proxy that uses a zonal network endpoint group containing one instance.
- D. Create a TCP proxy that uses backend services containing an instance group with two instances.

Correct Answer: A

Community vote distribution



Question #149 Topic 1

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 projects. Connect the VLAN attachment to the Shared VPC's host project.
- C. Use standalone projects, and deploy the VLAN attachments in the individual projects. Connect the VLAN attachment to the standalone projects' Dedicated Interconnects.
- D. Use standalone projects and deploy the VLAN attachments and Dedicated Interconnects in each of the individual projects.

Correct Answer: A

Community vote distribution



Question #150 Topic 1

You have several microservices running in a private subnet in an existing Virtual Private Cloud (VPC). You need to create additional serverless services that use Cloud Run and Cloud Functions to access the microservices. The network traffic volume between your serverless services and private microservices is low. However, each serverless service must be able to communicate with any of your microservices. You want to implement a solution that minimizes cost. What should you do?

- A. Deploy your serverless services to the serverless VPC. Peer the serverless service VPC to the existing VPC. Configure firewall rules to allow traffic between the serverless services and your existing microservices.
- B. Create a serverless VPC access connector for each serverless service. Configure the connectors to allow traffic between the serverless services and your existing microservices.
- C. Deploy your serverless services to the existing VPC. Configure firewall rules to allow traffic between the serverless services and your existing microservices.
- D. Create a serverless VPC access connector. Configure the serverless service to use the connector for communication to the microservices.

Correct Answer: D

Community vote distribution



Question #151 Topic 1

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

Correct Answer: BC

Community vote distribution



Question #152 Topic 1

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 routing. 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
- B. Use global routing. 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
- C. Use regional routing. 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

- D. Use global routing. 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

Correct Answer: D

Community vote distribution

D (68%)

B (32%)

Question #153 Topic 1

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 masterAuthorizedNetworksConfig. Configure kubectl to communicate with the endpoint 192.168.38.2.
- B. Add the network 192.168.38.0/28 to the masterAuthorizedNetworksConfig. Configure kubectl to communicate with the endpoint 192.168.38.2
- C. Add the network 192.168.36.0/24 to the masterAuthorizedNetworksConfig. Configure kubectl to communicate with the endpoint 192.168.38.2
- D. 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.

Correct Answer: A

Community vote distribution

A (100%)

Question #154 Topic 1

Your company's logo is published as an image file across multiple websites that are hosted by your company. You have implemented Cloud CDN; however, you want to improve the performance of the cache hit ratio associated with this image file. What should you do?

- A. Configure custom cache keys for the backend service that holds the image file, and clear the Host and Protocol checkboxes.
- B. Configure the default time to live (TTL) as 0 for the image file.
- C. Configure versioned URLs for each domain to serve users the image file before the cache entry expires.
- D. Configure Cloud Storage as a custom origin backend to host the image file, and select multi-region as the location type.

Correct Answer: A

Community vote distribution

A (100%)

Question #155 Topic 1

Your company recently migrated to Google Cloud in a single region. You configured separate Virtual Private Cloud (VPC) networks for two departments: Department A and Department B. Department A has requested access to resources that are part of Department B's VPC. You need to configure the traffic from private IP addresses to flow between the VPCs using multi-NIC virtual machines (VMs) to meet security requirements. Your configuration also must:

- Support both TCP and UDP protocols
- Provide fully automated failover
- Include health-checks
- Require minimal manual intervention in the client VMs

Which approach should you take?

- A. Create the VMs in the same zone, and configure static routes with IP addresses as next hops.
- B. Create the VMs in different zones, and configure static routes with instance names as next hops.
- C. Create an instance template and a managed instance group. Configure a single internal load balancer, and define a custom static route with the internal TCP/UDP load balancer as the next hop.
- D. Create an instance template and a managed instance group. Configure two separate internal TCP/UDP load balancers for each protocol (TCP/UDP), and configure the client VMs to use the internal load balancers' virtual IP addresses.

Correct Answer: C

Community vote distribution

C (60%)

D (40%)

Question #156 Topic 1

You are designing an IP address scheme for new private Google Kubernetes Engine (GKE) clusters. Due to IP address exhaustion of the RFC 1918 address space in your enterprise, you plan to use privately used public IP space for the new clusters. You want to follow Google-recommended practices. What should you do after designing your IP scheme?

- A. Create the minimum usable RFC 1918 primary and secondary subnet IP ranges for the clusters. Re-use the secondary address range for the pods across multiple private GKE clusters.
- B. Create the minimum usable RFC 1918 primary and secondary subnet IP ranges for the clusters, Re-use the secondary address range for the services across multiple private GKE clusters.
- C. Create privately used public IP primary and secondary subnet ranges for the clusters. Create a private GKE cluster with the following options selected: --enable-ip-alias and --enable-private-nodes.
- D. Create privately used public IP primary and secondary subnet ranges for the clusters. Create a private GKE cluster with the following options selected: --disable-default-snat, --enable-ip-alias, and --enable-private-nodes.

Correct Answer: D

Community vote distribution

D (75%)

C (25%)

Question #157 Topic 1

You want Cloud CDN to serve the `https://www.example.com/images/spacetime.png` static image file that is hosted in a private Cloud Storage bucket. You are using the `USE_ORIGIN_HEADERS` cache mode. You receive an HTTP 403 error when opening the file in your browser, and you see that the HTTP response has a `Cache-Control: private, max-age=0` header. How should you correct this issue?

- A. Enable negative caching for the backend bucket.
- B. Change the cache mode to Force cache all content.
- C. Configure a Cloud Storage bucket permission that gives allUsers the Storage Legacy Object Reader role.
- D. Increase the default time-to-live (TTL) for the backend service.

Correct Answer: C

Question #158 Topic 1

You are deploying an application that runs on Compute Engine instances. You need to determine how to expose your application to a new customer. You must ensure that your application meets the following requirements:

- Maps multiple existing reserved external IP addresses to the instance
- Processes IP Encapsulating Security Payload (ESP) traffic

What should you do?

- A. Configure a target pool, and create protocol forwarding rules for each external IP address.
- B. Configure a backend service, and create an external network load balancer for each external IP address.
- C. Configure a target instance, and create a protocol forwarding rule for each external IP address to be mapped to the instance.
- D. Configure the Compute Engine instances' network interface external IP address from None to Ephemeral. Add as many external IP addresses as required.

Correct Answer: C

Community vote distribution

C (55%)

A (45%)

Question #159 Topic 1

Your product team has web servers running on both `us-east1` and `us-west1` regions in the `prod-servers` project. Your security team plans to install an intrusion detection system (IDS) in their own Google Cloud project to inspect the incoming network traffic. What should you do?

- A. Create a new project and a VPC for the security team.
Peer the new VPC with the web servers' VPC in the `prod-servers` project.
Create an internal load balancer and the IDS system in both `us-east1` and `us-west1`.
Enable Packet Mirroring, and create packet mirroring policies inside the new project.
- C. Create a host project and a Shared VPC for the security team.
Make `prod-servers` a service project, and relocate the web servers to shared subnets in both regions.
Enable IP forwarding on all the web servers.
Create the IDS system in a non-shared subnet of `us-east1` or `us-west1`.
Configure the web servers to forward the packets to the IDS system.
- C. Create a new project and a VPC for the security team.
Peer the new VPC with the web servers' VPC in the `prod-servers` project.
Enable IP forwarding on all the web servers.

Install the IDS system in both us-east1 and us-west1.

Configure the web servers to forward the packets to the IDS system.

- D. Create a host project and a Shared VPC for the security team.

Make prod-servers a service project, and relocate the web servers to shared subnets in both regions.

Create an internal load balancer and the IDS system in a subnet in either us-east1 or us-west1.

Enable Packet Mirroring, and create a packet mirroring policy inside the host project.

Correct Answer: A

Community vote distribution

A (100%)

Question #160 Topic 1

You are in the process of deploying an internal HTTP(S) load balancer for your web server virtual machine (VM) instances. What two prerequisite tasks must be completed before creating the load balancer? (Choose two.)

- A. Choose a region.
- B. Create firewall rules for health checks.
- C. Reserve a static IP address for the load balancer.
- D. Determine the subnet mask for a proxy-only subnet.
- E. Determine the subnet mask for Serverless VPC Access.

Correct Answer: BD

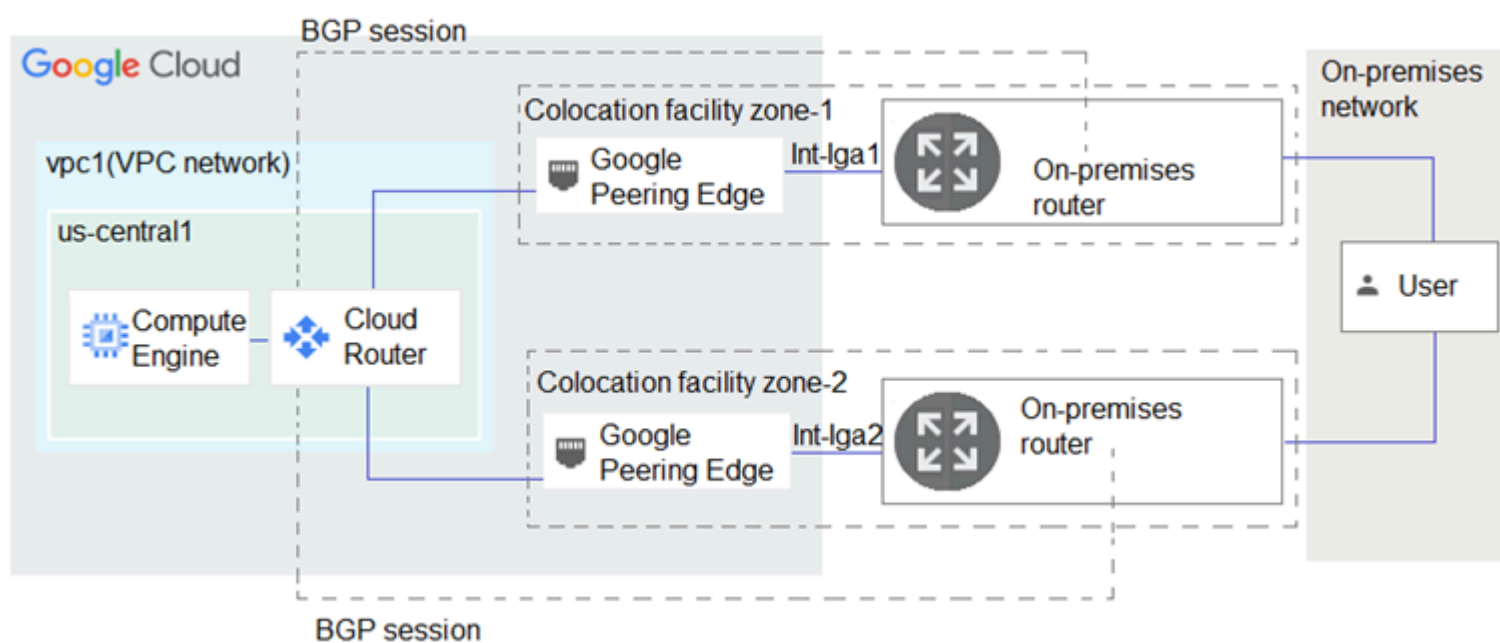
Community vote distribution

BD (71%)

AD (29%)

Question #161 Topic 1

You have the networking configuration shown in the diagram. A pair of redundant Dedicated Interconnect connections (int-lga1 and int-lga2) terminate on the same Cloud Router. The Interconnect connections terminate on two separate on-premises routers. You are advertising the same prefixes from the Border Gateway Protocol (BGP) sessions associated with the Dedicated Interconnect connections. You need to configure one connection as Active for both ingress and egress traffic. If the active Interconnect connection falls, you want the passive Interconnect connection to automatically begin routing all traffic. Which two actions should you take to meet this requirement? (Choose two.)



- A. Configure the advertised route priority as 200 for the BGP session associated with the active interconnect connection.
- B. Configure the advertised route priority > 10,200 on the active Interconnect connection.
- C. Advertise a lower MED on the active Interconnect connection from the on-premises router.
- D. Advertise a lower MED on the passive Interconnect connection from the on-premises router.
- E. Configure the advertised route priority as 200 for the BGP session associated with the passive Interconnect connection.

Correct Answer: CE

Community vote distribution

CE (67%)

AC (33%)

Question #162 Topic 1

You are a network administrator at your company planning a migration to Google Cloud and you need to finish the migration as quickly as possible. To ease the transition, you decided to use the same architecture as your on-premises network: a hub-and-spoke model. Your on-premises architecture consists of over 50 spokes. Each spoke does not have connectivity to the other spokes, and all traffic is sent through the hub for security reasons. You need to ensure that the Google Cloud architecture matches your on-premises architecture. You want to implement a solution that minimizes management overhead and cost, and uses default networking quotas and limits. What should you do?

- A. Connect all the spokes to the hub with Cloud VPN.
- B. Connect all the spokes to the hub with VPC Network Peering.
- C. Connect all the spokes to the hub with Cloud VPN. Use a third-party network appliance as a default gateway to prevent connectivity between the spokes.
- D. Connect all the spokes to the hub with VPC Network Peering. Use a third-party network appliance as a default gateway to prevent connectivity between the spokes.

Correct Answer: C

Community vote distribution

C (63%)

13%

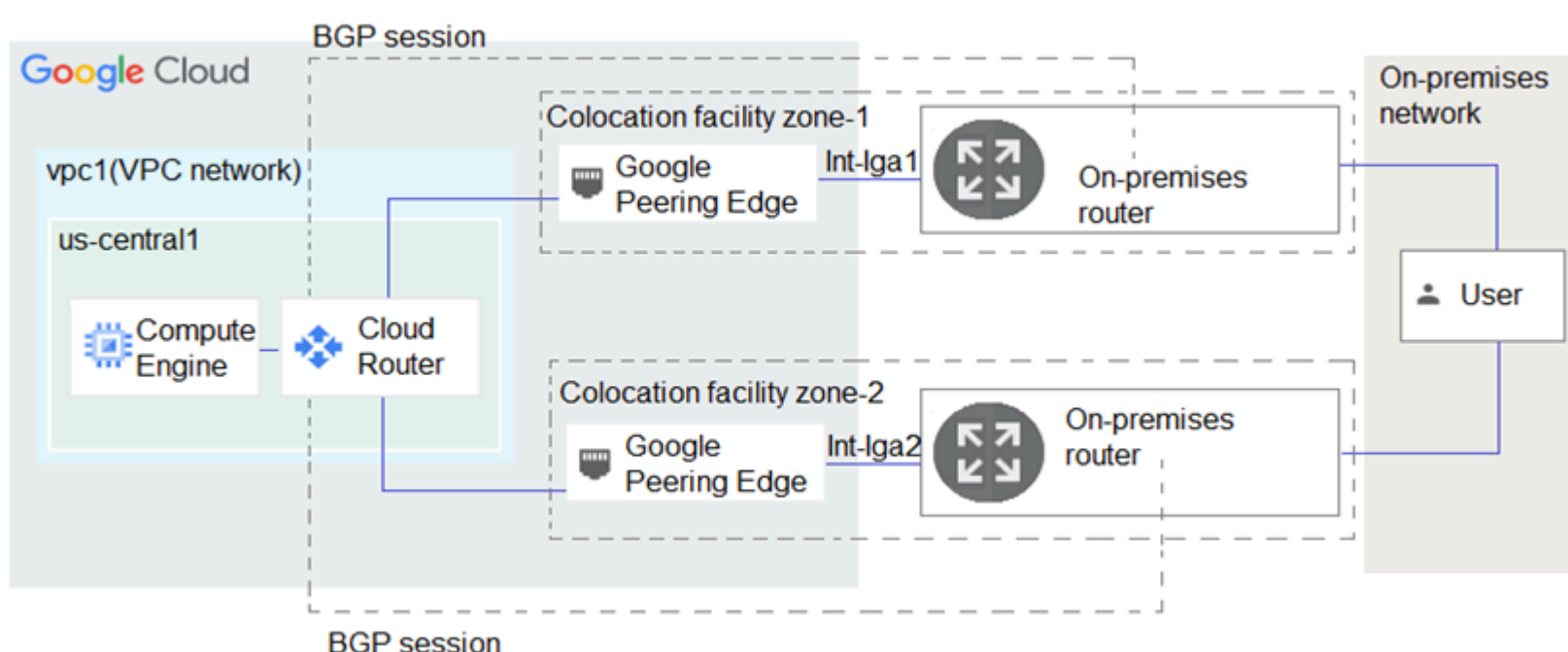
13%

13%

Question #163 Topic 1

You have the networking configuration shown in the diagram. Two VLAN attachments associated with two Dedicated Interconnect connections terminate on the same Cloud Router (mycloudrouter). The Interconnect connections terminate on two separate on-premises routers. You advertise the same prefixes from the Border Gateway Protocol (BGP) sessions associated with each of the VLAN attachments.

You notice an asymmetric traffic flow between the two Interconnect connections. Which of the following actions should you take to troubleshoot the asymmetric traffic flow?



- A. From the Google Cloud console, navigate to Cloud Logging to view VPC Flow Logs and review the results.
- B. From the Cloud CLI, run `gcloud compute --project PROJECT_ID routers get-status mycloudrouter --region REGION` and review the results.
- C. From the Google Cloud console, navigate to the Hybrid Connectivity, select the Cloud Router, and view BGP sessions.
- D. From the Cloud CLI, run `gcloud compute routers describe mycloudrouter --region REGION` and review the results.

Correct Answer: C

Community vote distribution

C (60%)

D (30%)

10%

Question #164 Topic 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: D*Community vote distribution*

D (80%)

A (20%)

Question #165 Topic 1

Your company is planning a migration to Google Kubernetes Engine. Your application team informed you that they require a minimum of 60 Pods per node and a maximum of 100 Pods per node. Which Pod per node CIDR range should you use?

- A. /24
- B. /25
- C. /26
- D. /28

Correct Answer: A*Community vote distribution*

A (100%)

Question #166 Topic 1

You are designing a packet mirroring policy as part of your network security architecture for your gaming workload. Your infrastructure is located in the us-west2 region and deployed across several zones: us-west2-a, us-west2-b, and us-west2-c. The infrastructure is running a web-based application on TCP ports 80 and 443 with other game servers that utilize the UDP protocol. You need to deploy packet mirroring policies and collector instances to monitor web application traffic while minimizing inter-zonal network egress costs.

Following Google-recommended practices, how should you deploy the packet mirroring policies and collector instances?

- A. Create three packet mirroring policies: one for each zone. Create one group of collector instances for the us-west2 region. Configure each packet mirroring policy to match traffic for its zone based on instance-tags, and create a filter for TCP traffic.
- B. Create one packet mirroring policy for the us-west2 region. Create one group of collector instances for the us-west2 region. Configure the packet mirroring policy to match traffic for web server instances based on instance-tags, and create a filter for TCP traffic.
- C. Create three packet mirroring policies: one for each zone. Create three groups of collector instances: one group for each zone. Configure each policy to match traffic for its zone based on instance-tags, and create a filter for TCP traffic.
- D. Create three packet mirroring policies: one for each zone. Create three groups of collector instances: one group for each zone. Configure each policy to match traffic for its zone based on subnets, and create a filter for TCP traffic.

Correct Answer: B

Community vote distribution



Question #167 Topic 1

Your company recently migrated to Google Cloud. You configured separate Virtual Private Cloud (VPC) networks for Department A and Department B. You need to configure both VPC networks to have access to the same on-premises location through separate links with full isolation between the VPC networks. Your design must also query on-premises DNS servers from workloads in Google Cloud using conditional forwarding. You want to minimize operational overhead. What should you do?

- A. Customize the operating system DNS configuration files to target the on-premises DNS servers.
- B. Keep the different VPC networks from both departments isolated with different on-premises links, and separate Cloud DNS private zones and Cloud DNS forwarding zones.
- C. Peer Department A's and Department B's VPC networks to have all on-premises connectivity via a single VPC network. Use separate Cloud DNS private zones and Cloud DNS forwarding zones.
- D. Configure a Cloud DNS Peering zone in Department A's VPC network pointing to Department B's VPC and a Cloud DNS outbound forwarding zone in Department B's VPC network. Use separate on-premises links in each VPC network.

Correct Answer: D

Community vote distribution



Question #168 Topic 1

You are planning to use Terraform to deploy the Google Cloud infrastructure for your company. The design must meet the following requirements:

- Each Google Cloud project must represent an internal project that your team will work on.
- After an internal project is finished, the infrastructure must be deleted.
- Each internal project must have its own Google Cloud project owner to manage the Google Cloud resources.
- You have 10-100 projects deployed at a time.

While you are writing the Terraform code, you need to ensure that the deployment is simple and the code is reusable with centralized management.

What should you do?

- A. Create a single project and single VPC for each internal project.
- B. Create a single Shared VPC and attach each Google Cloud project as a service project.
- C. Create a single project and additional VPCs for each internal project.
- D. Create a Shared VPC and service project for each internal project.

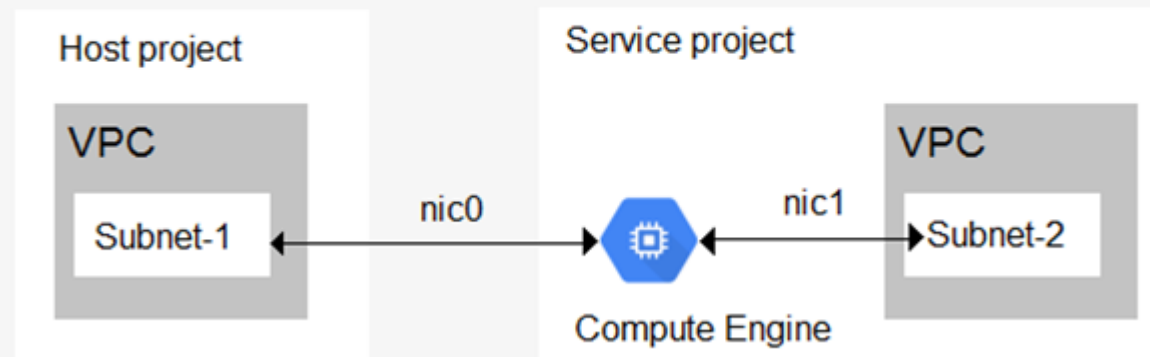
Correct Answer: B

Community vote distribution



Question #169 Topic 1

You have the following Shared VPC design. VPC Flow Logs is configured for Subnet-1 in the host VPC. You also want to monitor flow logs for Subnet-2. What should you do?



- A. Configure a VPC Flow Logs filter for Subnet-2 in the host project VPC.
- B. Configure VPC Flow Logs in the service project VPC for Subnet-2.
- C. Configure Packet Mirroring in both the host and service project VPCs.
- D. Configure a firewall rule to permit Subnet-2 IP addresses outbound in the host project VPC.

Correct Answer: A

Community vote distribution



Question #170 Topic 1

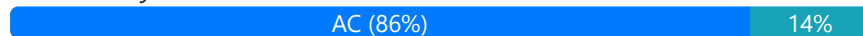
You are configuring your organization's Google Cloud environment to connect to your on-premises network, which does not support Border Gateway Protocol (BGP). Your on-premises network has 30 CIDR ranges that must be reachable from Google Cloud. Your VPN gateway creates a unique child security association (SA) per CIDR. You must ensure that the 30 CIDR ranges in your on-premises network are reachable from Google Cloud.

Following Google-recommended practices, which two methods can you use to accomplish this? (Choose two.)

- A. Create a single Cloud VPN tunnel that uses route-based VPN.
- B. Create a single Cloud VPN tunnel that uses policy-based routing with 30 CIDRs as the remote traffic selectors.
- C. Create multiple Cloud VPN tunnels that use policy-based routing so that each tunnel has one CIDR block for its local traffic selector and one CIDR block for its remote traffic selector. Connect each tunnel to unique peer IP addresses.
- D. Create multiple Cloud VPN tunnels that use policy-based routing with 10 CIDR per tunnel as the remote traffic selectors.
- E. Create multiple Cloud VPN tunnels that use policy-based routing so that each tunnel has one CIDR block for its local traffic selector and one CIDR block for its remote traffic selector. Connect each tunnel to the same peer IP address.

Correct Answer: AC

Community vote distribution



Question #171 Topic 1

You have two VPCs: VPC A in Project A and VPC B in Project B. The VPCs are peered, and each VPC has VM instances in four zones. You are using the Network Intelligence Center Performance Dashboard to investigate the packet loss for traffic flows that start in VPC A and terminate in VPC B. You need the reported packet loss metric to have at least a 90% confidence level. What should you do?

- A. Ensure that each zone in each of the VPC networks has at least 10 compute instances. Look in Project A for the reported metric.
- B. Ensure that each zone in each of the VPC networks has at least 9 compute instances. Look in Project B for the reported metric.
- C. Ensure that each zone in each of the VPC networks has at least 9 compute instances. Look in Project A for the reported metric.
- D. Ensure that each zone in each of the VPC networks has at least 10 compute instances. Look in Project B for the reported metric.

Correct Answer: D

Community vote distribution



Question #172 Topic 1

You are designing a new network infrastructure for your customer in Google Cloud. Your customer requires a connection between two Google Cloud VPCs that must include a VPN tunnel. You want to follow Google-recommended practices while ensuring maximum availability of the connection. Which VPN configuration should you choose?

- A. Policy-based VPN using Classic VPN between the two Google Cloud VPCs
- B. Border Gateway Protocol (BGP)-based VPN using Classic VPN between the two Google Cloud VPCs
- C. Route-based VPN using Classic VPN between the two Google Cloud VPCs
- D. Border Gateway Protocol (BGP)-based VPN using HA VPN between the two Google Cloud VPCs

Correct Answer: D

Community vote distribution

