Q1. You need to restrict access to your Google Cloud load-balanced application so that only specific IP addresses can connect.
What should you do?

A. Create a secure perimeter using the Access Context Manager feature of VPC Service Controls and restrict access to the source IP range of the allowed clients and Google health check IP ranges.

B. Create a secure perimeter using VPC Service Controls, and mark the load balancer as a service restricted to the source IP range of the allowed clients and Google health check IP ranges.

C. Tag the backend instances "application," and create a firewall rule with target tag "application" and the source IP range of the allowed clients and Google health check IP ranges.

D. Label the backend instances "application," and create a firewall rule with the target label "application" and the source IP range of the allowed clients and Google health check IP ranges.

Answer: C

Q2. 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.

Answer: D

Q3. 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.

Answer: C

Q4. You are migrating to Cloud DNS and want to import your BIND zone file.
Which command should you use?

A. gcloud dns record-sets import ZONE_FILE --zone MANAGED_ZONE

B. gcloud dns record-sets import ZONE_FILE --replace-origin-ns --zone MANAGED_ZONE

C. gcloud dns record-sets import ZONE_FILE --zone-file-format --zone MANAGED_ZONE

D. gcloud dns record-sets import ZONE_FILE --delete-all-existing --zone MANAGED ZONE

Answer: C

Q5. 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.

An: B

Explanation: auto mode will create group of duplicated subnets. 10.128.0.0/9 still collide with existing subnet in auto mode VPC

Q6. 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.

AN: AD

Explanation: PGA is enabled on the subnet used by the VM's network interface.

Q7. 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.

Answer: A

Q8. 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.

Answer: A

Explanation:
If ever needed for Virtual Private Cloud (VPC) sharing, deploy VLAN attachment and interconnect in the host project
Must always create VLAN attachments and Cloud Routers for an Interconnect connection only in the Shared VPC host project

Q9. 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

An: B

Q10. You created a new VPC network named Dev with a single subnet. You added a firewall rule for the network Dev to allow HTTP traffic only and enabled logging.
When you try to log in to an instance in the subnet via Remote Desktop Protocol, the login fails. You look for the Firewall rules logs in Stackdriver Logging, but you do not see any entries for blocked traffic. You want to see the logs for blocked traffic.

What should you do?

A. Check the VPC flow logs for the instance.

B. Try connecting to the instance via SSH, and check the logs.

C. Create a new firewall rule to allow traffic from port 22, and enable logs.

D. Create a new firewall rule with priority 65500 to deny all traffic, and enable logs.

Answer: D

Q11. 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.

Answer: A
Explanation: To be able to modify firewall rules, you required compute.securityAdmin role

Q12. 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.

Answer: B

Explanation: “Create a service” is wildly general. TCP Proxy. Global load balancer meant for HTTP or HTTPS only

Q13. 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.

Answer: D

Q14. 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.

Answer: BC

Explanation: Cloud DNS cannot manage interorganizational DNS queries

Q15. 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.

Answer: D

Q16. 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.

Answer: BD

Q17. 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.

Answer: B

Q18. 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.

Answer: B

Explanation:
Keyword: all requests go to server served by network load balancer. Network load balancer can use target pool

Q19. 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.

Answer: B

Explanation: With Cloud NAT, if instance is configured with external IP, precedence given to use external IP; so it won't be NATTED

Q20. You want to set up two Cloud Routers so that one has an active Border Gateway Protocol (BGP) session, and the other one acts as a standby.
Which BGP attribute should you use on your on-premises router?

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

Answer: D
Reference: aka MED

Q21. 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.

Answer: C

Q22. 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.

Answer: C
Reference: https://cloud.google.com/dns/docs/registrars#del-ds

Q23. You have an application hosted on a Compute Engine virtual machine instance that cannot communicate with a resource outside of its subnet. When you review the flow and firewall logs, you do not see any denied traffic listed.
During troubleshooting you find:
"¢ Flow logs are enabled for the VPC subnet, and all firewall rules are set to log.
"¢ The subnetwork logs are not excluded from Stackdriver.
"¢ The instance that is hosting the application can communicate outside the subnet.
"¢ Other instances within the subnet can communicate outside the subnet.
"¢ The external resource initiates communication.
What is the most likely cause of the missing log lines?

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

Answer: C

Q24. 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.

Answer: D

Explanation:
CDN will only compress in response generated by origin server.Presence of Via header indicates tha the request was forwarded by a proxy such as HTTP(S) load balancer

Q25. 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.

Answer: B

Explanation: Network LB is regional; hence can't disperse traffic accordingly. Use Global HTTP(s) is regional

Q26. You have an application running on Compute Engine that uses BigQuery to generate some results that are stored in Cloud Storage. You want to ensure that none of the application instances have external IP addresses.
Which two methods can you use to accomplish this? (Choose two.)

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

Answer: AE

Q27. 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.

Answer: D

Explanation: Google Best/Recommended practice is always create one VPC

Q28. You are adding steps to a working automation that uses a service account to authenticate. You need to drive the automation the ability to retrieve files from a Cloud Storage bucket. Your organization requires using the least privilege possible.

What should you do?

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

Answer: C

Q29. You converted an auto mode VPC network to custom mode. Since the conversion, some of your Cloud Deployment Manager templates are no longer working.
You want to resolve the problem.
What should you do?

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

Answer: D

Q30. You have recently been put in charge of managing identity and access management for your organization. You have several projects and want to use scripting and automation wherever possible. You want to grant the editor role to a project member.
Which two methods can you use to accomplish this? (Choose two.)

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

Answer: DE

Q31. 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].

Answer: A

Q32. You work for a multinational enterprise that is moving to GCP.
These are the cloud requirements:
"¢ An on-premises data center located in the United States in Oregon and New York with Dedicated Interconnects connected to Cloud regions us-west1 (primary HQ) and us-east4 (backup)
"¢ Multiple regional offices in Europe and APAC
"¢ Regional data processing is required in europe-west1 and australia-southeast1
"¢ Centralized Network Administration Team
Your security and compliance team requires a virtual inline security appliance to perform L7 inspection for URL filtering. You want to deploy the appliance in us- west1.
What should you do?

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

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

C. "¢ Create 1 VPC in a Shared VPC Host Project. "¢ Configure a 2-NIC instance in zone us-west1-a in the Host Project. "¢ Attach NIC0 in us-west1 subnet of the Host Project. "¢ Attach NIC1 in us-west1 subnet of the Host Project "¢ Deploy the instance. "¢ Configure the necessary routes and firewall rules to pass traffic through the instance.

D. "¢ Create 1 VPC in a Shared VPC Service Project. "¢ Configure a 2-NIC instance in zone us-west1-a in the Service Project. "¢ Attach NIC0 in us-west1 subnet of the Service Project. "¢ Attach NIC1 in us-west1 subnet of the Service Project "¢ Deploy the instance. "¢ Configure the necessary routes and firewall rules to pass traffic through the instance.

Answer: A

Keyword: VPC in Host Project, NIC to VPC

Q33. 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.

Answer: A
Explanation: Expected 100 nodes in subnet; using formula 2^c-4 = 100 → 7c → /25n

Q34. 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

Answer: D

Explanations:

SMTP and IMAP : rid of HTTPS
no SSL certificate, rid of SSL proxy.
globally, rid of Network

Q35. Your company is working with a partner to provide a solution for a customer. Both your company and the partner organization are using GCP. There are applications in the partner's network that need access to some resources in your company's VPC. There is no CIDR overlap between the VPCs.
Which two solutions can you implement to achieve the desired results without compromising the security? (Choose two.)

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

Answer: AC
Explanation: Both u and partner org using GCP. No Interconnect nor Cloud NAT

Q36. 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.

Answer: B

Q45. 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.

Answer: D
Explanation: To connect to the master node in k8s cluster; always enable thru master authorized network. There is public endpoint as well as private endpoint IP

Q47. You have created an HTTP(S) load balanced service. You need to verify that your backend instances are responding properly.

How should you configure the health check?

A. Set request-path to a specific URL used for health checking, and set proxy-header to PROXY_V1.

B. Set request-path to a specific URL used for health checking, and set host to include a custom host header that identifies the health check.

C. Set request-path to a specific URL used for health checking, and set response to a string that the backend service will always return in the response body.

D. Set proxy-header to the default value, and set host to include a custom host header that identifies the health check.

Answer: C

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

Q50. 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.

Answer: A
Explanations: Managed IG surely is built to autoscale

Q51. 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.

Answer: D
Keyword: invalidate

Q66. 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.

Answer: D

Q1. 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

Answer: B

Explanations: VPC-native cluster uses alias IP addresses address ranges.
From https://cloud.google.com/kubernetes-engine/docs/how-to/flexible-pod-cidr#overview

"With the *default* maximum of 110 Pods per node, Kubernetes assigns a /24 CIDR block (256 addresses) to each of the nodes."

That is, /24 for one node.
We have 3 nodes, so we need /22.

Q2. You are responsible for designing a new connectivity solution for your organization 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. Configure HA VPN in us-west1. Configure a Border Gateway Protocol (BGP) session between your Cloud Router and your on-premises data center.
B. Order a Direct Peering connection in the same metropolitan area. Configure Border Gateway Protocol (BGP) session between Google and your router.
C. Order a Carrier Peering connection in the same metropolitan area. Configure Border Gateway Protocol (BGP) session between Google and your router.
D. 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.

Answer: C

Explanations: Interconnect only access to resources in google cloud, hence it does not give you access to Google Workspace. However if CI is combined with PGA, then that gives access to supported Google APIs and products from on-premises.
Since we have service provider, carrier peering will be able to use that.

Q3. 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 existing VPC. Configure firewall rules to allow traffic between the serverless services and your existing microservices.
B. 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.
C. Create a serverless VPC access connector for each serverless service. Configure the connectors 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 connectors for communication to the microservices.

Answer: D

Explanation: Serverless VPC requires access connector configuration. One will do for all serverless services.

Q4. 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 2 answers

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

Answer: BE

Explanation If you use manual NAT IP address assignment to configure a Cloud NAT gateway, you can confidently share a set of common external source IP addresses with a destination party.
If you need to support more than 1,008 VMs, you can assign a second NAT IP address to the Cloud NAT gateway. With two NAT IP addresses, keeping the minimum number of ports per VM at 64, you can support 2,016 VMs:
Answer A cant get to 2000 VMs. Hence E will be correct

Q5. 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 Virtual Private Cloud (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 a default route, and use Cloud NAT to translate traffic from your on-premises network.
B. Configure the existing Cloud Routers to advertise the Google API's public virtual IP addresses.
C. Add Direct Peering links and use them for connectivity to Google APIs that use public virtual IP addresses.
D. Use Private Google Access for on-premises hosts with restricted googleapis.com virtual IP addresses.

Answer: D

Explanation: VPC Service control is configured with PGA . They are created on org, project or folder level.

Q6. 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 subnet.
B. Set the advertised routes to Global for the Cloud Router.
C. Configure each subnet's VPN connections to use Cloud VPN to connect to the branch office.
D. Configure the VPC dynamic routing mode to Global.

Answer: D

Explanation: Single VPN gateway with global dynamic routing mode

Q7. 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
    servicesIpv4CidrBlock:  192.168.37.0/24
    servicesSecondaryRangeName:  customer-1-svc
    useIpAliases: true

…
masterAuthorizedNetworkConfig:
…

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

…

serviceIpv4Cidr: 192.168.37.0/24

…

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 192.168.38.0/28 to the masterAuthorizedNetworksConfig. Configure kubectl to communicate with the endpoint 192.168.38.2.
B. 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.
C. Add the network 192.168.40.0/24 to the masterAuthorizedNetworksConfig. Configure kubectl to communicate with the endpoint 192.168.38.2.
D. Add the network 192.168.36.0/24 to the masterAuthorizedNetworksConfig. Configure kubectl to communicate with the endpoint 192.168.38.2.

Answer: C

Explanation: Main thing this VM is not configured with an external/public IP and with different subnet 192.168.40.0/24. Only answer C point to the instance network.

Q8. 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 the 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 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.
D. Configure VPC Flow logs. Review the logs by filtering on the source and destination.

Answer:

Explanation: A

NIC Connectivity Tests : " These tests also can be used to ensure the correct network security or compliance are being implemented properly "
NIC Network Topology just provide whole network diagram in a better visualisation

Q9. 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 2 answers

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

Answer: DE
Reference: Modify VLAN attachment only able to change maximum transmission unit (MTU) not the bandwidth . https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/modifying-vlan-attachments#gcloud
Apparently Link Aggregation Control Protocol (LACP) is configurable on Google interconnect.

Q10. You want to configure load balancing for an internet-facing, standard voice-over-IP (VOIP) application. Which type of load balancing should you use?

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

Answer: A

Explanation: Internet facing can't use option B and D. And C only meant for HTTP port 80 and port 443. VOIP uses standard network port of 5060

Q11. You have an HA VPN connection with two tunnels running in active/passive mode between your Virtual Private Cloud 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 Virtual Private Cloud (VPC).
C. Configure the maximum transmission unit (MTU) to its highest supported value.
D. Configure a second set of active/passive VPN tunnels.

Answer: D

Explanation: Each Cloud VPN tunnel support max upto 3 Gbps. To increase bandwidth, simply add another tunnel or another Gateway with additional tunnels.

Q12. 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 VPC Flow Logs. Create a sink in Cloud Logging to send filtered egress VPC Flow Logs to the IDS.
B. Create an internal HTTP(S) load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.
C. Create an internal TCP/UDP load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.
D. Enable firewall logging, and forward all filtered egress firewall logs to the IDS.

Answer: C

Explanations:

PM works with internal TCP/UDP only. See https://cloud.google.com/vpc/docs/packet-mirroring
VPC Flow Logs only records network flows sent from and received by virtual machines (VMs) instances
Firewall logging only records traffic denied/permit by firewall rules

Q13. 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 Virtual Private Cloud (VPC). Create service project 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, one VPC for Database. Use Virtual Private Cloud (VPC) Network Peering to connect all VPCs in full mesh.

Answer: A

Explanation: With Shared VPC, you only need to create one host project and attach one or more other service projects to it.

Q14. You recently noticed a recurring daily spike in network usage in your Google Cloud project. You need to identify the virtual machines (VMs) 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.

Answer: A

Explanation : VPC Flow Logs only records network flows sent from and received by virtual machines (VMs) instances
Firewall logging only analyze effects of firewall rules
PM works with external monitoring tools such as IDS . See
https://cloud.google.com/vpc/docs/packet-mirroring

Q15. Your organization has a single project that contains multiple Virtual Private Cloud (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 network. What should you do?

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

Answer: C

Explanations: Service control perimeters are configured at an organization, folder or project level.

Q16. 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 standalone projects and deploy the VLAN attachments and Dedicated Interconnect in each of the individual projects.
B. Use standalone projects and deploy the VLAN attachments in the individual projects. Connect the VLAN attachment to the standalone projects' Dedicated Interconnects.
C. Use Shared VPC, and deploy the attachments in the service projects. Connect the VLAN attachment to the Shared VPC's host project.
D. Use Shared VPC, and deploy the VLAN attachments and Dedicated Interconnect in the host project.

Answer: D

Explanation: Based on Google best practices: In Shared VPC, configure all VLAN attachments, not physical CI (ports) in the host projects

Q17. You have the following firewall ruleset applied to all instances in 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 role 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.

Answer: A
Explanations: To be able to modify fw rules, that required compute.securityAdmin role. This is confirm thru another question 😜

Q18. You recently deployed Compute Engine instances in region 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. Change the instance's network interface external IP address from None to Ephemeral.
B. Create a Cloud NAT gateway and Cloud Router in both us-west1 and us-east1.
C. Create a firewall rule that allows egress to destination 0.0.0.0/0.
D. Create a single global Cloud NAT gateway and global Cloud Router in the VPC.

Answer: B

Explanation: Cloud NAT gateway is configured on region level. There is no such thing as global NAT gateway.

Q19. 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 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.

Answer: A

Explanation: Changing VPC routing mode to global is needed if you have multiple regions in Google Cloud Virtual Private Cloud (VPC). In this case, we only focus on one region : us-west1
Option C: Why the additional Cloud Router …

Q20. 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. 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.
B. 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 ip DNS server as the alternative DNS Server.
C. 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.
D. 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.

Answer: C

Explanations: Your on-premises network must have a route to the 35.199.192.0/19 destination with the next hop being a VPN tunnel or Interconnect connection for the same VPC network that sent the DNS request.

Refer to https://cloud.google.com/dns/docs/best-practices#best_practices_for_dns_forwarding_zones_and_server_policies

Q21. 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 TCP proxy that uses a zonal network endpoint group containing one instance.
B. Create a network load balancer that uses a target pool backend with two instances.
C. Create a TCP proxy that uses backend services containing an instance group with two instances.
D. Create a network load balancer that uses backend services containing one instance group with two instances.

Answer: D

Explanations: Network load balancer with target pool backend does not support IPv6: hence we need to use instance group
Very tricky; there is TCP Proxy load balancer, but the answer choice come short at TCP proxy only.

Q22. 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?

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

Answer: DE

Explanations: Most load balancers use non-legacy health checks, with exception of target pool-based Network load balancer requires legacy health checks.
Definitely, you won't find health check option in VPC network section

Q23. 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 regions. Configure a round-robin A record in Cloud DNS.
B. Deploy the Cloud Run services to multiple availability zones. Create a global TCP load balancer. Add the Cloud Run endpoints to its backend service.
C. 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.
D. 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.

Answer: C

Explanation: Cloud Run is regional and managed by Google to be redundantly available across all the zones within that region. Meaning to say, you can't select which zone to deploy Cloud Run
Cloud Endpoints is tool for API development

Q24. 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. Configure 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 and import on all projects' VPC networks.

Answer: A

Explanation: Can a VLAN attachments shared across projects? Yes
Key is multiple VPCs exists in each projects.

Q25. Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from on-premises locations using Cloud Interconnect connections. Your company must be able to send traffic to Cloud Storage only through the Interconnect links while accessing other Google APIs and services over the public internet. What should you do?

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

Answer: B

Explanation: Private Google Access doesn't support virtual machines (VMs) with both internal and external IP configured. Though with Private service Connect, there is private.googleapis.com as well as restricted.googleapis.com

Q26. 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 Border Gateway Protocol (BGP) session?

A.

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

B.

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	169.254.0.254	169.254.20.2	65002
router-2	if-tunnel-b-to-a-if-0	169.254.0.254	169.254.20.1	65001

C.

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

D.

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

Answer: A

Explanation: Definitely using 169.254.x.y between the BGP gateway IP addresses. And has to be unique IP addresses on both router

Q27. You are responsible for configure 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 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 address with priority 1.
B. 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 address 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 address 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 address with priority 0.

Answer: B

Explanations: Hierarchical firewall policy only applicable to Organization or folder level not on Virtual Private Cloud (VPC) networks (which uses VPC Firewall Policy). Hierarchical firewall policy overrides VPC firewall policies.
Again, lowest number is higher priority

Q28. 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 Google Cloud Armor security policy, and create a policy rule to allow 203.0.113.1/32.
B. Configure a firewall rule accepting 203.0.113.1/32, and set a target tag equal to VPN_GATEWAY_1.
C. 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.
D. Configure the Resource Manager constraint constraints/compute.restrictVpnPeerIPs to use an allowList consisting of only the 203.0.113.1/32 address.

Answer: D

References: https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints

Q29. Your organization is implementing a new security policy to control how firewall rules are applied to control flows between virtual machines (VMs). Using Google-recommend 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 exists in the VPC. Which firewall rule should you configure to allow only this communication path?

A.
- Firewall rule direction: ingress
- Action: allow
- Target: specific VM B tag
- Source ranges: VM A tag and VM A source IP address
- Priority: 1000

B.
- Firewall rule direction: ingress
- Action: allow
- Target: specific VM A tag
- Source ranges: VM B tag and VM B source IP address
- Priority: 100

C.
- Firewall rule direction: ingress
- Action: allow
- Target: VM B service account
- Source ranges: VM A service account
- Priority: 1000

D.
- 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

Answer: A

Explanations: According to documentation as well as configuration, to configure ingress firewall rule, you need to specify only the source. For egress, specify destination or target.
See https://cloud.google.com/vpc/docs/using-firewalls

Q30. 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 networks 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 an internal TCP/UDP load balancer with the two network virtual appliances as backends.
   Configure two routes for 10.0.0.0/8 with different priorities, each pointing to separate network virtual appliances.
B. Configure two routes for 10.0.0.0/8 with different priorities, each pointing to separate network virtual appliances.
C. Configure a network load balancer with 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 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.

Answer: A

Explanation: Network load balancer is a regional load balancer that is able to distribute traffic from the internet. Furthermore scenarios requires failover capability instead of load sharing.

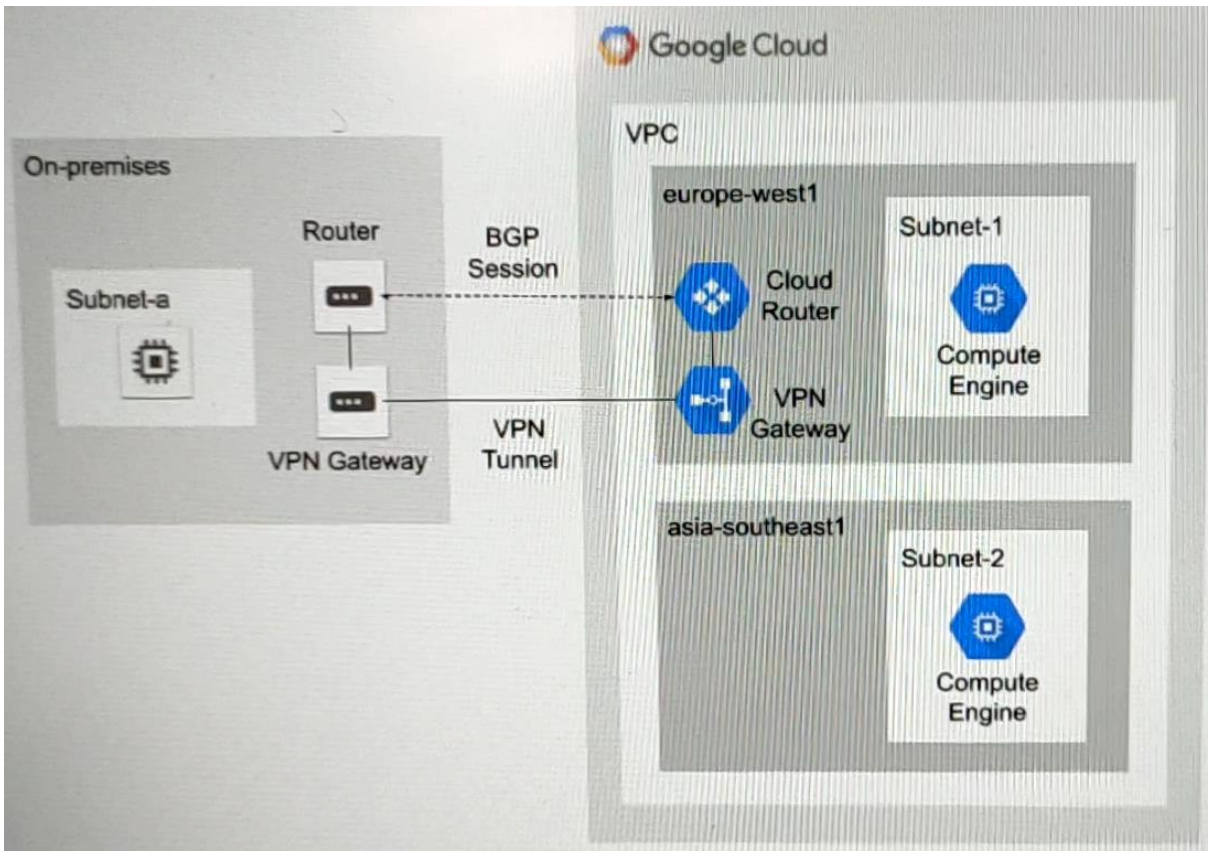
Q31. You are designing a hybrid cloud environment for your organization. Your Google Cloud environment is interconnected with your on-premises network using Cloud HA VPN and Cloud Router. The Cloud Router is configured with the default settings. Your on-premises DNS server is located at 192.168.20.88 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 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.
B. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that point 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.
C. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that point 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.
D. 1. Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that point 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.

Answer: C

Explanations: Must configure on-premises firewall to allow incoming and outgoing traffic to 35.199.192.0/19. VM from VPC will query Cloud DNS and gets forwarded to the local DNS in on-prem. So answer B and D is wrong.

Q32. 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. Add a second Border Gateway Protocol (BGP) session to the Cloud Router.
B. Enable IP forwarding in the asia-southeast1 region.
C. Configure a custom route advertisement on the Cloud Router.
D. Change the VPC dynamic routing mode to Global.

Answer: D

Explanation: The dynamic routing mode of the VPC network controls whether the advertised subnet IP address ranges only come from the same region as the Cloud Router or whether they come from all regions:

Q33. 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 routes are being advertised over the VPN tunnel. Which filter should you use in Cloud Logging to examine the logs?

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

Answer: D

Explanation: refer to https://cloud.google.com/network-connectivity/docs/router/how-to/viewing-logs-metrics or google "monitoring metrics for cloud router"

Q34. 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. 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.
B. Review the VPC audit logs in Cloud Logging for the affected instances.
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.

Answer: C
Keyword: You need to validate network misconfiguration !

Q35. 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 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.
B. 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.
C. 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.
D. 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.

Answer: C
Explanation: Regional vs Global. Multi-region must use global. That get rid of option B and D .
By setting us-east1 to 1000 will ensure us-west1 connection to be ranked 1 (priority default to 100)

Q36. You suspected 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 virtual machines (VMs) to understand where the traffic is coming from. What should you do?

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

Answer: A

Explanation:
When enable VPC Flow Logs , you enable for all VMs in a subnet.
Data Access audit logs is enabled for your Google Cloud resources and services:
Refer to https://cloud.google.com/vpc/docs/using-flow-logs#enabling-vpc-flow-logs

Q37. 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 VPC firewall rule that denies traffic, enable logging, set enforcement to disabled, and review the necessary logs.
B. Create a Google Cloud Armor policy that denies traffic, and review the necessary logs.
C. Create a VPC firewall rule that denies traffic, enable logging, set enforcement to enabled, and review the necessary logs.
D. Create a Google Cloud Armor policy that denies traffic, enable preview mode, and review the necessary logs

Answer: D

Explanations: With load balancer combined with Cloud Armor that can defends against malicious attack such as DDOS. And with preview mode, we identify but not really enforcing it.

Q37b. Your company offers a popular gaming service. Your instances are deployed with private IP addresses, and external access is granted through a global load balancer. You have recently engaged a traffic-scrubbing service and want to restrict your origin to allow connections only from the traffic-scrubbing service.

What should you do?

A. Create a Cloud Armor Security Policy that blocks all traffic except for the traffic-scrubbing service.

B. Create a VPC Firewall rule that blocks all traffic except for the traffic-scrubbing service.

C. Create a VPC Service Control Perimeter that blocks all traffic except for the traffic-scrubbing service.

D. Create IPTables firewall rules that block all traffic except for the traffic-scrubbing service.

Answer: A

Q38. 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. Create a new route in the spoke VPC that points to IP address 10.0.0.5.

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.
   4. Import the custom routes in the spokes.

C. 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 of the spokes.

D. 1. Create two default routes in the hub VPC that points 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.

Answer: C

Explanation: In hub-to-spoke VPC Peering, we shall export route from hub and import route from spoke. Due to the requirement to "must use the hub's virtual appliances for internet, we must delete default internet gateway of the spokes too.

Q39. You are responsible for enabling Private Google Access for the virtual machines (VMs) 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. 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.

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 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.

C. 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 with a CNAME for *.googleapis.com to private.googleapis.com, and create a CNAME 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.
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.

Answer: B

Explanation: https://cloud.google.com/vpc/docs/configure-private-google-access#config

C option is wrong bcos you must create DNS zone for googleapis.com
D option is wrong bcos we must use private.googleapis.com restricted.googleapis.com only routable from within google cloud
Between A and B. A seems wrong bcos lower priority means traffic wont' come to on-premises.

Q40. 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 may 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 visible to the backends. What configuration should you use?

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

Answer: D

Explanations: X-Forwarded-For help you identify the IP addresses of clients when use HTTP(S) load balancer

Q41. 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 requirements?

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

Answer: D

Max Nodes = 10 nodes

Max pods = 8 pods x 10 = 80 . c = 7 , n = 25

Max services = 1024 svc . 2^c-2 = 1024 so means 2^c = 1026 , n = 21

Q42. 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 Virtual Private Cloud (VPC) to handle HTTP and HTTPS web traffic for TCP only. What should you do?

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

Answer: C

Explanations:

Rule created for HTTP (80) and HTTPS (443)
Egress is outgoing traffic from VPC, ingress is correct choice

Q43. 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 Cloud Storage as a custom origin backend to host the image file, and select multi-region as the location type.
C. Configure versioned URLs for each domain to serve users the image file before the cache entry expires.
D. Configure the default time to live (TTL) as 0 for the image file.

Answer: A

Explanation: Custom cache keys

Q44. 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 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 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-rule \
--allow TCP:3306 \
--source-service-accounts sa-app@democloud-idp-demo.iam.gserviceaccount.com \
--target-service-accounts sa-db@my-project.iam.gserviceaccount.com

B. 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

C. Create network tags 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 tcp:3306 \
--source-tags app-server \
--target-service-accounts sa-db@my-project.iam.gserviceaccount.com

D. 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-rule \
--allow TCP:3306 \
--source-ranges 10.120.0.0/20 \
--source-service-accounts sa-app@democloud-idp-demo.iam.gserviceaccount.com \
--target-service-accounts sa-db@my-project.iam.gserviceaccount.com

Answer: B

Explanation:

Subnet-a (10.128.0.0/20) – database servers

Subnet-b (172.16.0.0/24) – application and web servers

Configure firewall to allow application server → database query → database servers

https://cloud.google.com/vpc/docs/firewalls#service-accounts-vs-tags

Option A: wrong source service account.
Option C and D is invalid. If uses target service account, can't use source tags or combination of source IP ranges and source tags.

Q45. 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 Router. 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 Router.
C. Create a GKE private cluster with a private endpoint for the control plane. Configure authorized networks to specify the desired on-premises subnets.
D. Create a GKE public cluster. Configure authorized networks to specify the desired on-premises subnets.

Answer: C

Explanation:

Option A and B is invalid – bcos connectivity with on-premises is already in place and we do not create VPC Peering between google cloud and on-premises
Option D is invalid – public is wrong

Q46. 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 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 Sales VPC.
B. Create a VPC Network Peering connection between the Finance VPC and Sales VPC.
C. Configure the instances that require communication between each other with an external IP addresses.
D. Configure Cloud NAT and a Cloud Router in Sales and Finance VPC.

Answer: B

Q47. 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 VPC firewall ruleset, and apply it to all instances in unmanaged instance groups.
B. Create a Google Cloud Armor policy, and apply it to a backend service that uses an internet network endpoint group (NEG) backend.
C. Create a hierarchical firewall ruleset, and apply it to the VPC's parent organization resource node.
D. Create a Google Cloud Armor policy, and apply it to a backend service that uses an unmanaged instance group backend.

Answer: D

Explanation: Definitely Cloud Armor, however NEG not supported

Q48. 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 Virtual Private Cloud (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.

Answer: C

Go for C; bcos physically should be close to massive user traffic (us-east4)

Q49. 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 instances 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. Create a hub and spoke VPN deployment in each spoke VPC to connect back to 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. 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.

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. 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 VPCs, with the hub VPC as the target.
3. Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.

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 on-premises network directly

Answer: B

Explanation:
A and D uses VPN to connect . But why
C is wrong due to non-creation of VPC Peering

Q50. 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 overlapping RFC 1918 ranges with multiple isolated VPC networks.
B. Use non-RFC 1918 ranges with a single global VPC.
C. Use overlapping RFC 1918 ranges with multiple isolated VPC networks and Cloud NAT.
D. Use multiple VPC networks with a transit network using VPC Network Peering.

Answer:

Q51. 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

Answer: D

Explanation: It's a UDP traffic! Network load balancer can direct TCP or UDP across regional backends

Q52. 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

Answer: C

Q53. You need to establish network connectivity between three Virtual Private Cloud networks, Sales, Marketing, and Finance, so that users can access resources in all three VPCs. You configure VPC peering between the Sales VPC and the Finance VPC. You also configure VPC peering between the Marketing VPC and the Finance VPC. After you complete the configuration, some users cannot connect to resources in the Sales VPC and the Marketing VPC. You want to resolve the problem.

What should you do?

A. Configure VPC peering in a full mesh.

B. Alter the routing table to resolve the asymmetric route.

C. Create network tags to allow connectivity between all three VPCs.

D. Delete the legacy network and recreate it to allow transitive peering.

Answer: A
Explanations: Virtual Private Cloud (VPC) peering is not transitive.

Q54. our 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.

Answer: AC
Explanation: DDOS definitely go for Cloud Armor. And in synergy it works great with Global load balancer

Q55. 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

Answer: D

Q56. 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

Answer: D
Explanation: Cannot run Border Gateway Protocol (BGP) >hence we need Partner IC with layer 3

Q57. 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

Answer: AB

Q58. 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.

Answer: AC
Explanation: Private Service access require private connection. That require use the Service Networking API . Refers to https://cloud.google.com/service-infrastructure/docs/enabling-private-services-access

Q59. 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.

Answer: A

Q60. 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.

Answer: A

Q61. You are deploying a global external TCP load balancing solution and want to preserve the source IP address of the original layer 3 payload.

Which type of load balancer should you use?

A. HTTP(S) load balancer

B. Network load balancer

C. Internal load balancer

D. TCP/SSL proxy load balancer

Answer: B

Q62. 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.

Answer: A
Reference: https://cloud.google.com/load-balancing/docs/url-map-concepts#pm-constraints

Q63. 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.

Answer: AE

Q64. 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

Answer: C

Q65. You need to ensure your personal SSH key works on every instance in your project. You want to accomplish this as efficiently as possible.

What should you do?

A. Upload your public ssh key to the project Metadata.

B. Upload your public ssh key to each instance Metadata.

C. Create a custom Google Compute Engine image with your public ssh key embedded.

D. Use gcloud compute ssh to automatically copy your public ssh key to the instance.

Answer: A
Reference: https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#addkey

Q66. 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.

Answer: D
Reference: https://cloud.google.com/compute/docs/instance-groups/rolling-out-updates-to-managed-instance-groups

Q67. 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.

Answer: BD
Explanations: Minimize Cost: Just Share Virtual Private Cloud (VPC), and with that firewall rules to allow traffic.

Q68. 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.

Answer: B

Q69. ou 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.

Answer: B

Q70. 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.

Answer: A

Q71. 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.

Answer: C

Q72. You are using the gcloud command line tool to create a new custom role in a project by coping a predefined role. You receive this error message:

INVALID_ARGUMENT: Permission resourcemanager.projects.list is not valid

What should you do?

A. Add the resourcemanager.projects.get permission, and try again.

B. Try again with a different role with a new name but the same permissions.

C. Remove the resourcemanager.projects.list permission, and try again.

D. Add the resourcemanager.projects.setIamPolicy permission, and try again.

Answer: C
Explanation: Can't create custom role at project level

Q73. You want to use Partner Interconnect to connect your on-premises network with your VPC. You already have an Interconnect partner.

What should you first?

A. Log in to your partner's portal and request the VLAN attachment there.

B. Ask your Interconnect partner to provision a physical connection to Google.

C. Create a Partner Interconnect type VLAN attachment in the GCP Console and retrieve the pairing key.

D. Run gcloud compute interconnect attachments partner update <attachment> / --region <region> --admin-enabled.

Answer: C

Q74. 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

Answer: A

Q75. You need to create a GKE cluster in an existing VPC that is accessible from on-premises. You must meet the following requirements:

☞ IP ranges for pods and services must be as small as possible.

☞ The nodes and the master must not be reachable from the internet.

☞ You must be able to use kubectl commands from on-premises subnets to manage the cluster.

How should you create the GKE cluster?

A. "¢ Create a private cluster that uses VPC advanced routes. "¢ Set the pod and service ranges as /24. "¢ Set up a network proxy to access the master.

B. "¢ Create a VPC-native GKE cluster using GKE-managed IP ranges. "¢ Set the pod IP range as /21 and service IP range as /24. "¢ Set up a network proxy to access the master.

C. "¢ Create a VPC-native GKE cluster using user-managed IP ranges. "¢ Enable a GKE cluster network policy, set the pod and service ranges as /24. "¢ Set up a network proxy to access the master. "¢ Enable master authorized networks.

D. "¢ Create a VPC-native GKE cluster using user-managed IP ranges. "¢ Enable privateEndpoint on the cluster master. "¢ Set the pod and service ranges as /24. "¢ Set up a network proxy to access the master. "¢ Enable master authorized networks.

Answer: D
Explanations: By default, clusters can access the controller through its private endpoint, and authorized networks can be defined within the VPC network.
https://cloud.google.com/solutions/creating-kubernetes-engine-private-clusters-with-net-proxies

Q76. 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.

Answer: C

Q77. After a network change window one of your company's applications stops working. The application uses an on-premises database server that no longer receives any traffic from the application. The database server IP address is 10.2.1.25. You examine the change request, and the only change is that 3 additional VPC subnets were created. The new VPC subnets created are 10.1.0.0/16, 10.2.0.0/16, and 10.3.1.0/24/ The on-premises router is advertising 10.0.0.0/8.

What is the most likely cause of this problem?

A. The less specific VPC subnet route is taking priority.

B. The more specific VPC subnet route is taking priority.

C. The on-premises router is not advertising a route for the database server.

D. A cloud firewall rule that blocks traffic to the on-premises database server was created during the change.

Answer: B

Q78. 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.

Answer: C
Explanation: Just create one, and SSH is using 22/TCP. EZpz

Q79. You are configuring a new instance of Cloud Router in your Organization's Google Cloud environment to allow connection across a new Dedicated Interconnect to your data center Sales, Marketing, and IT each have a service project attached to the Organization's host project.

Where should you create the Cloud Router instance?

A. VPC network in all projects

B. VPC network in the IT Project

C. VPC network in the Host Project

D. VPC network in the Sales, Marketing, and IT Projects

Answer: C
Explanation: Definitely in the host project!

Q80. You want to establish a dedicated connection to Google that can access Cloud SQL via a public IP address and that does not require a third-party service provider.

Which connection type should you choose?

A. Carrier Peering

B. Direct Peering

C. Dedicated Interconnect

D. Partner Interconnect

Answer: B
Explanation: Keywords: dedicated connection and public IP addresses : Direct Peering it is!

Q81. You need to enable Cloud CDN for all the objects inside a storage bucket. You want to ensure that all the object in the storage bucket can be served by the CDN.

What should you do in the GCP Console?

A. Create a new cloud storage bucket, and then enable Cloud CDN on it.

B. Create a new TCP load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.

C. Create a new SSL proxy load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.

D. Create a new HTTP load balancer, select the storage bucket as a backend, enable Cloud CDN on the backend, and make sure each object inside the storage bucket is shared publicly.

Answer: D
Explanation: Always remember CDN needs Global HTTP(s) load balancer

Q82. You need to configure a static route to an on-premises resource behind a Cloud VPN gateway that is configured for policy-based routing using the gcloud command.

Which next hop should you choose?

A. The default internet gateway

B. The IP address of the Cloud VPN gateway

C. The name and region of the Cloud VPN tunnel

D. The IP address of the instance on the remote side of the VPN tunnel

Answer: C
Reference: https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns

Q83. 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 addresses

Answer: B
Reference: https://cloud.google.com/vpc/docs/add-remove-network-tags

Q84. 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.

Answer: B
Ref: https://cloud.google.com/compute/docs/access/iam#compute.networkAdmin

Q85. With the help of a partner, you deployed G Suite last year and have seen the rapid pace of innovation and development within the platform. Your CIO has requested that you develop a method of staying up-to-date on all things G Suite so that you can be prepared to take advantage of new features and ensure that your organization gets the most out of the platform.

What should you do?

A. Develop a cadence of regular roadmap and business reviews with your partner.

B. Regularly scan the admin console and keep track of any new features you identify.

C. Create a Feature Release alert in the Alert Center to be alerted to new functionality.

D. Put half of your organization on the Rapid Release Schedule to highlight differences.

Answer: A

Q86.