

Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer

<https://www.2passeasy.com/dumps/Professional-Cloud-Network-Engineer/>



NEW QUESTION 1

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

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

Answer: D

NEW QUESTION 2

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

- A. Deploy the Cloud Run services to multiple availability zone
- B. Create a global TCP load balance
- C. Add the Cloud Run endpoints to its backend service.
- D. Deploy the Cloud Run services to multiple region
- E. Create serverless network endpoint groups (NEGs) that point to the service
- F. Create a global HTTPS load balancer, and attach the serverless NEGs as backend services of the load balancer.
- G. Deploy the Cloud Run services to multiple availability zone
- H. Create Cloud Endpoints that point to the service
- I. Create a global HTTPS load balancer, and attach the Cloud Endpoints to its backend
- J. Deploy the Cloud Run services to multiple region
- K. Configure a round-robin A record in Cloud DNS.

Answer: B

NEW QUESTION 3

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

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

Answer: C

NEW QUESTION 4

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:

<https://cloud.google.com/dns/docs/best-practices>

NEW QUESTION 5

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

Answer: B

NEW QUESTION 6

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

Answer: D

Explanation:

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

NEW QUESTION 7

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: DE

Explanation:

<https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/retrieving-loas>

NEW QUESTION 8

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

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

Answer: D

NEW QUESTION 9

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:

https://cloud.google.com/kubernetes-engine/docs/how-to/private-clusters#cant_reach_cluster <https://cloud.google.com/kubernetes-engine/docs/how-to/authorized-networks>

NEW QUESTION 10

You are responsible for configuring firewall policies for your company in Google Cloud. Your security team has a strict set of requirements that must be met to configure firewall rules. Always allow Secure Shell (SSH) from your corporate IP address. Restrict SSH access from all other IP addresses. There are multiple projects and VPCs in your Google Cloud organization. You need to ensure that other VPC firewall rules cannot bypass the security team's requirements. What should you do?

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

Answer: A

NEW QUESTION 10

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

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

Answer: D

Explanation:

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

<https://cloud.google.com/cdn/docs/setting-up-cdn-with-bucket>

NEW QUESTION 14

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

NEW QUESTION 15

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

Explanation:

<https://cloud.google.com/solutions/tcp-optimization-for-network-performance-in-gcp-and-hybrid> <https://cloud.google.com/solutions/tcp-optimization-for-network-performance-in-gcp-and-hybrid>

<https://cloud.google.com/blog/products/gcp/5-steps-to-better-gcp-network-performance?hl=ml>

NEW QUESTION 17

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

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

Answer: B

NEW QUESTION 18

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

- A. Use the Network Intelligence Center Connectivity Tests to test the connectivity between the VPC and the on-premises network.
- B. Use Network Intelligence Center Network Topology to check the traffic flow, and replay the traffic from the time period when the connectivity issue occurred.
- C. Configure VPC Flow Log
- D. Review the logs by filtering on the source and destination.
- E. 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.

Answer: B

NEW QUESTION 21

You have an application running on Compute Engine that uses BigQuery to generate some results that are stored in Cloud Storage. You want to ensure that none of the application instances have external IP addresses.

Which two methods can you use to accomplish this? (Choose two.)

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

Answer: AE

Explanation:

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

NEW QUESTION 22

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

NEW QUESTION 25

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

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

Answer: C

NEW QUESTION 26

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

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

Answer: C

NEW QUESTION 31

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

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

Answer: A

NEW QUESTION 34

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

- A. Create a secure perimeter using the Access Context Manager feature of VPC Service Controls and restrict access to the source IP range of the allowed clients and Google health check IP ranges.
- B. Create a secure perimeter using VPC Service Controls, and mark the load balancer as a service restricted to the source IP range of the allowed clients and Google health check IP ranges.
- C. Tag the backend instances "application," and create a firewall rule with target tag "application" and the source IP range of the allowed clients and Google health check IP ranges.
- D. Label the backend instances "application," and create a firewall rule with the target label "application" and the source IP range of the allowed clients and Google health check IP ranges.

Answer: C

Explanation:

<https://cloud.google.com/load-balancing/docs/https/setting-up-https#sendtraffic>

NEW QUESTION 36

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

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

Answer: C

Explanation:

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

NEW QUESTION 40

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:

<https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview>

For Layer 3 connections, your service provider establishes a BGP session between your Cloud Routers and their edge routers for each VLAN attachment. You don't need to configure BGP on your on-premises router. Google and your service provider automatically set the correct configurations.

<https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview#connectivity-type>

NEW QUESTION 45

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

Explanation:

https://cloud.google.com/vpc/docs/firewall-rules-logging#egress_deny_example

You can only enable Firewall Rules Logging for rules in a Virtual Private Cloud (VPC) network. Legacy networks are not supported. Firewall Rules Logging only records TCP and UDP connections. Although you can create a firewall rule applicable to other protocols, you cannot log their connections. You cannot enable Firewall Rules Logging for the implied deny ingress and implied allow egress rules. Log entries are written from the perspective of virtual machine (VM) instances. Log entries are only created if a firewall rule has logging enabled and if the rule applies to traffic sent to or from the VM. Entries are created according to the connection logging limits on a best effort basis. The number of connections that can be logged in a given interval is based on the machine type. Changes to firewall rules can be viewed in VPC audit logs. <https://cloud.google.com/vpc/docs/firewall-rules-logging#specifications>

NEW QUESTION 47

You work for a university that is migrating to Google Cloud.

These are the cloud requirements:

On-premises connectivity with 10 Gbps Lowest latency access to the cloud Centralized Networking Administration Team

New departments are asking for on-premises connectivity to their projects. You want to deploy the most cost-efficient interconnect solution for connecting the campus to Google Cloud.

What should you do?

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

Answer: A

NEW QUESTION 51

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

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

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

Answer: A

NEW QUESTION 56

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

NEW QUESTION 58

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

A. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

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

B. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

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

C. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

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

D. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

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

Answer: C

NEW QUESTION 59

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

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

Answer: C

Explanation:

<https://cloud.google.com/sdk/gcloud/reference/dns/record-sets/import>

NEW QUESTION 60

Your company has just launched a new critical revenue-generating web application. You deployed the application for scalability using managed instance groups, autoscaling, and a network load balancer as frontend. One day, you notice severe bursty traffic that has caused autoscaling to reach the maximum number of instances, and users of your application cannot complete transactions. After an investigation, you think it is 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.
 E. The attack will stop when the application is offline.
 F. SSH into the backend compute engine instances, and view the auth logs and syslogs to further understand the nature of the attack.

Answer: BE

NEW QUESTION 62

Your company has defined a resource hierarchy that includes a parent folder with subfolders for each department. Each department defines their respective project and VPC in the assigned folder and has the appropriate permissions to create Google Cloud firewall rules. The VPCs should not allow traffic to flow

between them. You need to block all traffic from any source, including other VPCs, and delegate only the intra-VPC firewall rules to the respective departments. What should you do?

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

Answer: B

NEW QUESTION 63

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

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

Answer: D

NEW QUESTION 67

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

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

Answer: B

NEW QUESTION 70

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

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

Answer: B

NEW QUESTION 73

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

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

- A. Create a default route in the hub VPC that points to IP address 10.0.0.5. Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway. Export the custom routes in the hu
- B. Import the custom routes in the spokes.
- C. Create a default route in the hub VPC that points to IP address 10.0.0.5. Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway. Export the custom routes in the hu
- D. Import the custom routes in the spoke
- E. Delete the default internet gateway route of the spokes.
- F. Create two default routes in the hub VPC that point to the next hop instances of the virtual appliances. Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway. Export the custom routes in the hu
- G. Import the custom routes in the spokes.
- H. Create a default route in the hub VPC that points to IP address 10.0.0.5. Delete the default internet gateway route in the hub VPC, and create a new higher-priority route that is tagged only to the appliances with a next hop of the default internet gateway. Create a new route in the spoke VPC that points to IP address 10.0.0.5.

Answer: B

NEW QUESTION 74

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

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

Answer: D

Explanation:

<https://cloud.google.com/interconnect/docs/how-to/dedicated/creating-vlan-attachments>

NEW QUESTION 78

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

- A. Delete the default route in your VPC. Create a private Cloud DNS zone for googleapis.com, create a CNAME for *.googleapis.com to restricted googleapis.com, and create an A record for restricted googleapis.com that resolves to the addresses in 199.36.153.4/30. Create a static route in your VPC for the range 199.36.153.4/30 with the default internet gateway as the next hop.
- B. Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP). Create a public Cloud DNS zone with a CNAME for *.google.com to private googleapis.com, create a CNAME for * googleapis.com to private googleapis.com, and create an A record for Private googleapis.com that resolves to the addresses in 199.36.153.8/30. Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.
- C. Configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP) with a lower priority (MED) than the default VPC route. Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googleapis.com to private googleapis.com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30. Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.
- D. Delete the default route in your VPC and configure your on-premises router to advertise 0.0.0.0/0 via Border Gateway Protocol (BGP). Create a private Cloud DNS zone for googleapis.com, create a CNAME for * googleapis.com to Private googleapis.com, and create an A record for private.googleapis.com that resolves to the addresses in 199.36.153.8/30. Create a static route in your VPC for the range 199.36.153.8/30 with the default internet gateway as the next hop.

Answer: C

NEW QUESTION 79

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
- B. Configure VPC Networking Peering export/import routes and custom route advertisements on the Cloud Router
- C. Configure authorized networks to specify the desired on-premises subnets.
- D. Create a GKE private cluster with a public endpoint for the control plane
- E. Configure VPC Networking Peering export/import routes and custom route advertisements on the Cloud Routers.
- F. Create a GKE private cluster with a private endpoint for the control plane
- G. Configure authorized networks to specify the desired on-premises subnets.
- H. Create a GKE public cluster
- I. Configure authorized networks to specify the desired on-premises subnets.

Answer: C

NEW QUESTION 84

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

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

Answer: C

NEW QUESTION 89

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

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

Answer: B

NEW QUESTION 92

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

NEW QUESTION 96

You work for a multinational enterprise that is moving to GCP. These are the cloud requirements:

- An on-premises data center located in the United States in Oregon and New York with Dedicated Interconnects connected to Cloud regions us-west1 (primary HQ) and us-east4 (backup)
- Multiple regional offices in Europe and APAC
- Regional data processing is required in europe-west1 and australia-southeast1
- Centralized Network Administration Team

Your security and compliance team requires a virtual inline security appliance to perform L7 inspection for URL filtering. You want to deploy the appliance in us-west1.

What should you do?

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

Answer: B

Explanation:

<https://cloud.google.com/vpc/docs/shared-vpc>

NEW QUESTION 99

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

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

Answer: A

NEW QUESTION 100

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: A

NEW QUESTION 104

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: C

Explanation:

<https://cloud.google.com/load-balancing/docs/load-balancing-overview> mentions to use global load balancer for IPv6 termination.

NEW QUESTION 108

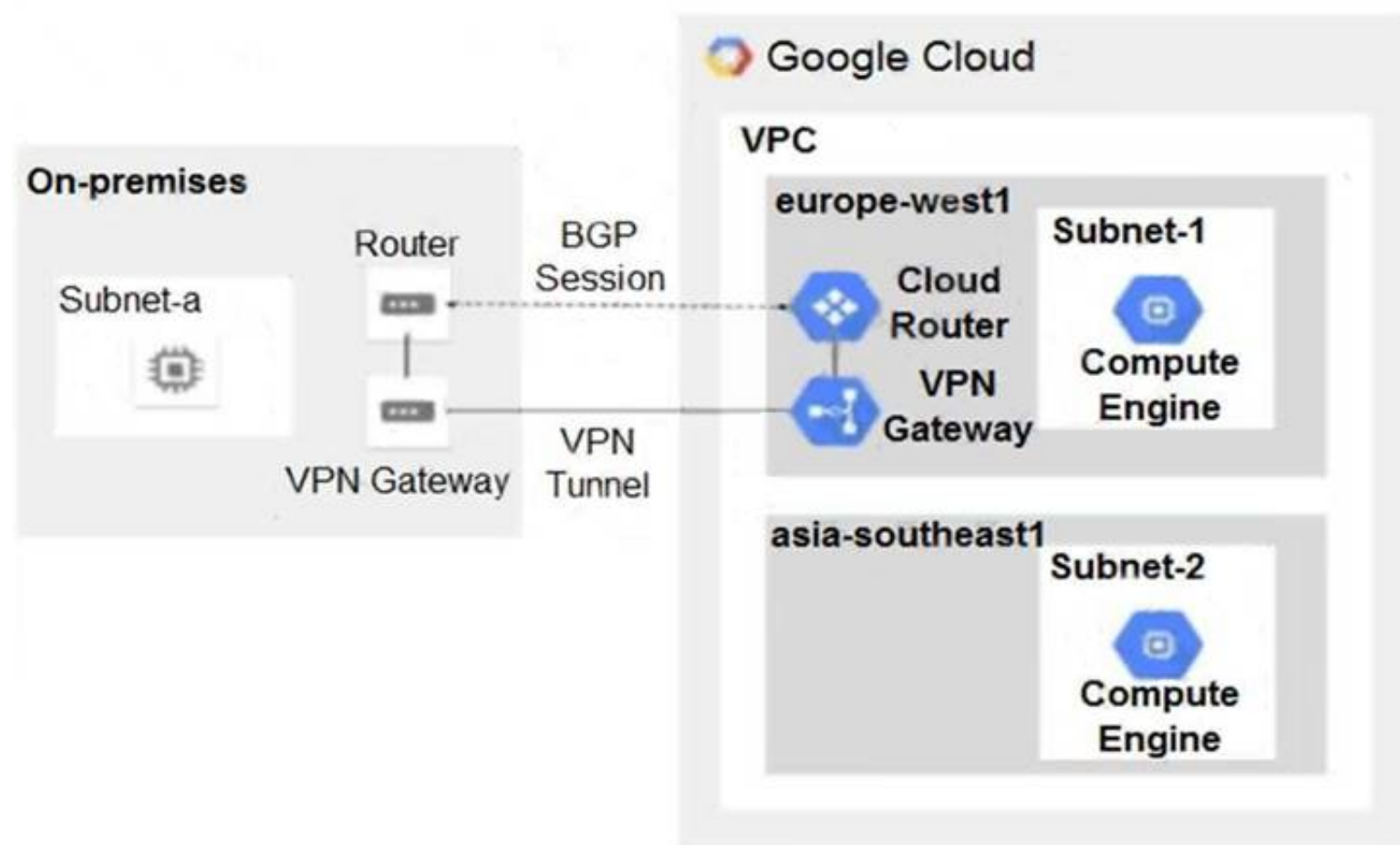
You have an HA VPN connection with two tunnels running in active/passive mode between your Virtual Private Cloud (VPC) and on-premises network. Traffic over the connection has recently increased from 1 gigabit per second (Gbps) to 4 Gbps, and you notice that packets are being dropped. You need to configure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

- A. Configure the remote autonomous system number (ASN) to 4096.
- B. Configure a second Cloud Router to scale bandwidth in and out of the VPC.
- C. Configure the maximum transmission unit (MTU) to its highest supported value.
- D. Configure a second set of active/passive VPN tunnels.

Answer: D

NEW QUESTION 109

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



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

Answer: C

NEW QUESTION 111

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

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

Answer: C

NEW QUESTION 113

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

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

Answer: D

NEW QUESTION 115

You are planning a large application deployment in Google Cloud that includes on-premises connectivity. The application requires direct connectivity between

workloads in all regions and on-premises locations without address translation, but all RFC 1918 ranges are already in use in the on-premises locations. What should you do?

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

Answer: D

NEW QUESTION 119

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

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

Answer: B

NEW QUESTION 123

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

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

Answer: C

NEW QUESTION 126

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

Answer: D

NEW QUESTION 127

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

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

Answer: A

NEW QUESTION 128

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

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

Answer: C

NEW QUESTION 132

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: CE

Explanation:

https://cloud.google.com/sql/docs/mysql/configure-private-services-access#console_1

C: If you are using private IP for any of your Cloud SQL instances, you only need to configure private services access one time for every Google Cloud project that has or needs to connect to a Cloud SQL instance. If your Google Cloud project has a Cloud SQL instance, you can either configure it yourself or let Cloud SQL do it for you to use private IP. Cloud SQL configures private services access for you when all the conditions below are true:

https://cloud.google.com/sql/docs/postgres/configure-private-services-access#before_you_begin

E: You can enable Private Google access on a subnet level and any VMs on that subnet can access Google APIs by using their internal IP address.

<https://cloud.google.com/vpc/docs/configure-private-google-access>

NEW QUESTION 137

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

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

Answer: B

NEW QUESTION 139

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

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

Answer: C

NEW QUESTION 141

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

Answer: A

NEW QUESTION 144

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

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

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

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

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

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

NEW QUESTION 148

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

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

Answer: A

NEW QUESTION 152

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

Answer: A

Explanation:

The service range setting is permanent and cannot be changed. Please see

<https://stackoverflow.com/questions/60957040/how-to-increase-the-service-address-range-of-a-gke-cluster> I think the correc tanswer is A since: Grow is expected to up to 100 nodes (that would be /25), then up to 200 pods per node (100 times 200 = 20000 so /17 is 32768), then 1500 services in a /21 (up to 2048)
<https://docs.netgate.com/pfsense/en/latest/book/network/understanding-cidr-subnet-mask-notation.html>

NEW QUESTION 156

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

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

Answer: C

NEW QUESTION 160

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

Explanation:

Direct Interconnect will be too expensive and also an overkill for this requirement. Managing multiple tunnels that too with packet loss consideration is complex also. Whereas partner interconnect fits the bill with providing required bandwidth but not super expensive also once setup not too complex too manage.

NEW QUESTION 164

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

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

Answer: B

NEW QUESTION 166

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

- A. Create network tag app-server and service account sa-db@my-project.iam.gserviceaccount.co
- B. Add the tag to the application servers, and associate the service account with the database server
- C. Run the following command: `gcloud compute firewall-rules create app-db-firewall-rule --action allow --direction ingress --rules top:3306 --source-tags app-server --target-service-accounts sa-db@my-project.iam.gserviceaccount.com`
- D. Create service accounts sa-app@my-project.iam.gserviceaccount.com and sa-db@my-project.iam.gserviceaccount.co
- E. Associate service account sa-app with the application servers, and associate the service account sa-db with the database server
- F. Run the following command: `gcloud compute firewall-rules create app-db-firewall-rule --allow TCP:3306 --source-service-accounts sa-app@my-project.iam.gserviceaccount.com --target-service-accounts sa-db@my-project.iam.gserviceaccount.com`
- G. Create service accounts sa-app@my-project.iam.gserviceaccount.com and sa-db@my-project.iam.gserviceaccount.co
- H. Associate the service account sa-app with the application servers, and associate the service account sa-db with the database server
- I. Run the following command: `gcloud compute firewall-rules create app-db-firewall-rule --allow TCP:3306 --source-ranges 10.128.0.0/20 --source-service-accounts sa-app@my-project.iam.gserviceaccount.com --target-service-accounts sa-db@my-project.iam.gserviceaccount.com`
- J. Create network tags app-server and db-server
- K. Add the app-server tag to the application servers, and add the db-server tag to the database server
- L. 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`

Answer: D

NEW QUESTION 171

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

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

Answer: B

NEW QUESTION 176

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

- A. Configure a host project with a Shared VPC
- B. Create service projects for Web, App, and Database.
- C. Configure one VPC for Web, one VPC for App, and one VPC for Database
- D. Configure HA VPN between each VPC.

- E. Configure three Shared VPC host projects, each with a service project: one for Web, one for App, and one for Database.
- F. Configure one VPC for Web, one VPC for App, and one VPC for Databases.
- G. Use VPC Network Peering to connect all VPCs in a full mesh.

Answer: C

NEW QUESTION 180

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

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

Answer: C

NEW QUESTION 185

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.
- D. 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.
- E. Add a second Cloud VPN gateway in a different region than the existing VPN gateway.
- F. 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

Explanation:

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#redundancy-options>

NEW QUESTION 187

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

Explanation:

https://cloud.google.com/load-balancing/docs/url-map#configuring_url_maps

Path matcher constraints Path matchers and path rules have the following constraints: A path rule can only include a wildcard character (*) after a forward slash character (/). For example, /videos/* and /videos/hd/* are valid for path rules, but /videos* and /videos/hd* are not. Path rules do not use regular expression or substring matching. For example, path rules for either /videos/hd or /videos/hd/* do not apply to a URL with the path /video/hd-abcd. However, a path rule for /video/* does apply to that path. <https://cloud.google.com/load-balancing/docs/url-map-concepts#pm-constraints>

NEW QUESTION 192

You have configured a Compute Engine virtual machine instance as a NAT gateway. You execute the following command:

```
gcloud compute routes create no-ip-internet-route \
--network custom-network1 \
--destination-range 0.0.0.0/0 \
--next-hop instance nat-gateway \
--next-hop instance-zone us-central1-a \
--tags no-ip --priority 800
```

You want existing instances to use the new NAT gateway. Which command should you execute?

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

Answer: B

Explanation:

<https://cloud.google.com/sdk/gcloud/reference/compute/routes/create>

In order to apply a route to an existing instance we should use a tag to bind the route to it.

NEW QUESTION 193

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.

Answer: AD

Explanation:

<https://cloud.google.com/vpc/docs/private-access-options#pga> Private Google Access VM instances that only have internal IP addresses (no external IP addresses) can use Private Google Access. They can reach the _external IP addresses_ of Google APIs and services.

NEW QUESTION 196

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

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

Answer: CE

NEW QUESTION 200

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Professional-Cloud-Network-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Professional-Cloud-Network-Engineer Product From:

<https://www.2passeasy.com/dumps/Professional-Cloud-Network-Engineer/>

Money Back Guarantee

Professional-Cloud-Network-Engineer Practice Exam Features:

- * Professional-Cloud-Network-Engineer Questions and Answers Updated Frequently
- * Professional-Cloud-Network-Engineer Practice Questions Verified by Expert Senior Certified Staff
- * Professional-Cloud-Network-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * Professional-Cloud-Network-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year