



CompTIA

CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.

Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates

First attempt guaranteed success.

<https://www.CertyIQ.com>

About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertyIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

<https://www.certyiq.com>

[Mail us on - certyiqofficial@gmail.com](mailto:certyiqofficial@gmail.com)



Lifetime Free Updates

We provide lifetime free updates to our customers. To make life easier for our valued customers and fulfill their needs



Free Exam PDF

You are sure to pass the exam completely free of charge



Money Back Guarantee

We Provide 100% money back guarantee to our customer in case of any failure

John

October 19, 2022



Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

Dana

September 04, 2022



Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Ahamed Shibly

2 months ago



Customer support is really fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!

October 22, 2022



Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study. Thank You certyiq team!

Henry Rome

2 months ago



These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago



Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's. Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

Google

(Professional Cloud Network Engineer)

Professional Cloud Network Engineer

Total: **172 Questions**

Link: <https://certyiq.com/papers?provider=google&exam=professional-cloud-network-engineer>

Question: 1

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

What should you do?

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

Answer: C

Explanation:

Answer C.

This question is actually asking specifically about using firewall with a Network LB, because Network Load Balancing is a pass-through load balancer, you control access to the load balancer's backends using Google Cloud firewall rules.

Reference:

https://link.springer.com/chapter/10.1007/978-1-4842-1004-8_4

Question: 2

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

Explanation:

VPC Network Peering enables you to peer VPC networks so that workloads in different VPC networks can communicate in private RFC 1918 space. Traffic stays within Google's network and doesn't traverse the public internet.

Reference:

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

Question: 3**CertyIQ**

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**Explanation:**

A. Not correct. Shared VPC work to connect resources from different project. Since requirements state "single project for 3 separate departments", shared VPC would not work here.

B. Not correct since Cloud VPN is used to connect peer networks traffic over Internet.

C. Correct.

D. Possible but it would incur in operational overhead if we compare with C.

Question: 4**CertyIQ**

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:**

Once you have the exported file from your other provider, you can use the `gcloud dns record-sets import` command to import it into your managed zone.

To import record-sets, you use the `dns record-sets import` command. The `--zone-file-format` flag tells import to expect a BIND zone formatted file. If you omit this flag, import expects a YAML-formatted records file.

Reference:

<https://medium.com/@prashantapaudel/gcp-certification-series-2-4-planning-and-configuring-network-resources-8045ac2cc2ac>

Question: 5**CertyIQ**

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.

Answer: B

Explanation:

B is correct answer, existing subnet can not be in range of C i.e. 10.128.0.0/9.

Reference:

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

Question: 6

CertyIQ

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:

A and D due to By default, when a Compute Engine VM lacks an external IP address assigned to its network interface, it can only send packets to other internal IP address destinations. You can allow these VMs to connect to the set of external IP addresses used by Google APIs and services by enabling Private Google Access on the subnet used by the VM's network interface. <https://cloud.google.com/vpc/docs/configure-private-google-access>

Question: 7

CertyIQ

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

Explanation:

Correct answer A . D is incorrect - it mentions that you are adding the ssh key to the project, but the question says "block project-wide SSH keys." therefore that ssh key will not be added to the instance.

Question: 8

CertyIQ

You work for a university that is migrating to GCP.

These are the cloud requirements:

"Ç On-premises connectivity with 10 Gbps

"Ç Lowest latency access to the cloud

"Ç 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:

Correct Answer is (A)

Using Cloud Interconnect with Shared VPC

You can use Shared VPC to share your VLAN attachment in a project with other VPC networks.

Choosing Shared VPC is preferable if you need to create many projects and would like to prevent individual project owners from managing their connectivity back to your on-premises network.

In this scenario, the host project contains a common Shared VPC network usable by VMs in service projects.

Because VMs in the service projects use this network, Service Project Admins don't need to create other VLAN

attachments or Cloud Routers in the service projects.

In this scenario, you must create VLAN attachments and Cloud Routers for a Cloud Interconnect connection only in the Shared VPC host project. The combination of a VLAN attachment and its associated Cloud Router are unique to a given Shared VPC network.

https://cloud.google.com/network-connectivity/docs/interconnect/how-to/enabling-multiple-networks-access-same-attachment#using_with

Question: 9

CertyIQ

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

Explanation:

The correct answer is B

HTTP/S port 80/443

TFTP port 69

Session affinity, (sticky sessions), overrides the load-balancing algorithm by directing all requests in a session to a specific application server.

So, we need a Session affinity by Client IP.

Session affinity

https://cloud.google.com/load-balancing/docs/backend-service#session_affinity

Session affinity options

https://cloud.google.com/load-balancing/docs/internal#session_affinity

The answer A&D produces the same (Client IP, protocol, and port) by the way.

Question: 10

CertyIQ

You created a new VPC network named Dev with a single subnet. You added a firewall rule for the network Dev to allow HTTP traffic only and enabled logging.

When you try to log in to an instance in the subnet via Remote Desktop Protocol, the login fails. You look for the Firewall rules logs in Stackdriver Logging, but you do not see any entries for blocked traffic. You want to see the logs for blocked traffic.

What should you do?

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

Answer: D

Explanation:

answer is D. implicit deny cant show logs you have to add new log with deny.

Question: 11

CertyIQ

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:

Answer is A: A Shared VPC Admin can define a Security Admin by granting an IAM member the Security Admin (compute.securityAdmin) role to the host project. Security Admins manage firewall rules and SSL certificates.

Reference:

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

Question: 12

CertyIQ

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:

Answer is C Use global load balancing when your backends are distributed across multiple regions, your users need access to the same applications and content, and you want to provide access by using a single anycast IP address. Global load balancing can also provide IPv6 termination.

Question: 13

CertyIQ

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: B

Explanation:

Correct answer is B, select to any IP address (0.0.0.0/0) is not recommended solution.

The answer is : B If you check the settings for route based configuration you will find that you cant select local selectors and only provide remote address list. and as all answers provide the following sentence : "Configure the appropriate local and remote traffic selectors". This eliminates answer D as you cant select local selectors on route based VPN. "Route-based VPN. When you use the Google Cloud console to create a route-based VPN, you only specify a list of remote IP ranges. Those ranges are used only to create routes in your VPC network to peer resources."

Question: 14

CertyIQ

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:

B and C will be the answer. If it says Cloud DNS I would go with D since zone transfer is unavailable. But based on the current situation both organizations have customized DNS and that means you may have both DNS use

Question: 15

CertyIQ

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:

- "Ç Each on-premises router is configured with a unique ASN.
- "Ç Each on-premises router is configured with the same routes and priorities.
- "Ç Both on-premises routers are configured with a VPN connected to a single Cloud Router.
- "Ç BGP sessions are established between both on-premises routers and the Cloud Router.
- "Ç 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

Explanation:

Cloud Router doesn't use ECMP across routes with different origin ASNs

For cases where you have multiple on-premises routers connected to a single Cloud Router, the Cloud Router learns and propagates routes from the router with the lowest ASN. Cloud Router ignores advertised routes from routers with higher ASNs, which might result in unexpected behavior. For example, you might have two on-premises routers advertise routes that are using two different Cloud VPN tunnels. You expect traffic to be load balanced between the tunnels, but Google Cloud uses only one of the tunnels because Cloud Router only propagated routes from the on-premises router with the lower ASN.

reference: <https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting#ecmp>

Question: 16

CertyIQ

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

Explanation:

Correct Answer is: B and D

Retrieve LOA-CFAs After you order a Dedicated Interconnect connection, Google sends you and the NOC (technical contact) an email with your Letter of Authorization and Connecting Facility Assignment (LOA-CFA) (one PDF file per connection). You must send these LOA-CFAs to your vendor so that they can install your connections. If you don't, your connections won't get connected.

Question: 17

CertyIQ

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

Explanation:

The Global External Load Balancer is a proxy, so the only way to see origin its is from Cloud Armor. Answer is B

Question: 18

CertyIQ

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:

Answer is B

'External TCP/UDP Network Load Balancing can use either a backend service or a target pool to define the group of backend instances that receive incoming traffic'

'Target pools work with forwarding rules that handle TCP and UDP traffic. You must create a target pool

before you can use it with a forwarding rule.'

Reference:

<https://cloud.google.com/compute/docs/instance-groups/adding-an-instance-group-to-a-load-balancer>

<https://cloud.google.com/load-balancing/docs/target-pools>

Question: 19

CertyIQ

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:

An external IP address has been configured on the instance.

Reference:

<https://www.sovereignsolutionscorp.com/google-cloud-nat/>

Question: 20

CertyIQ

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

Explanation:

Answer is D.

You can configure 2 different MED values for each BGP neighbor in your single on-prem router, to influence ISP(GCP)'s 2 separate routers to select which path they send traffic towards you. The lower MED value is preferred.

Reference:

<https://cloud.google.com/router/docs/concepts/overview>

Question: 21

CertyIQ

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

Explanation:

The answer is C.

Based on the answer options, this question is testing our understanding about Classic Cloud VPN, which is already deprecated, not HA VPN, which was released in May 2019.

Classic VPN is not possible to create 2 VPN tunnels within the same cloud VPN gateway to the same destination VPN gateway. so, B is wrong.

There are 3 options to increase bandwidth throughput.

1. Scale on-premises VPN gateway: using 1 Cloud VPN Gateway and 2 or more On-prem Gateways. Create a 2nd tunnel on your existing cloud VPN gateway that forwards the same IP range, but pointing at the second on-premises gateway. Cloud VPN gateway automatically load balances between the configured tunnels. You can set up the VPN Gateways to have multiple tunnels load balanced this way to increase the aggregate VPN connectivity throughput. Thus, C is correct.

Question: 22

CertyIQ

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

Explanation:

Before disabling DNSSEC for a managed zone you want to use, you must deactivate DNSSEC at your domain registrar to ensure that DNSSEC-validating resolvers can still resolve names in the zone.

Reference:

Question: 23

CertyIQ

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:

- "Ç Flow logs are enabled for the VPC subnet, and all firewall rules are set to log.
- "Ç The subnetwork logs are not excluded from Stackdriver.
- "Ç The instance that is hosting the application can communicate outside the subnet.
- "Ç Other instances within the subnet can communicate outside the subnet.
- "Ç 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

Explanation:

C is the right answer. The traffic is not matching the expected ingress rule, thus it will fall to the IMPLICIT DENY INGRESS RULE which is never logged.

Question: 24

CertyIQ

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:

If responses served by Cloud CDN are not compressed but should be, check that the web server software running on your instances is configured to compress responses. By default, some web server software will automatically disable compression for requests that include a Via header. The presence of a Via header indicates the request was forwarded by a proxy. HTTP proxies such as HTTP(S) load balancing add a Via header to each request as required by the HTTP specification. To enable compression, you may have to override your web server's default configuration to tell it to compress responses even if the request had a Via header.

Reference:

<https://cloud.google.com/cdn/docs/troubleshooting-steps>

Question: 25**CertyIQ**

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:**

Answer is B.

Network LB is regional service. This scenario requires global scale type of LB, thus HTTP LB is the correct choice.

Reference:

<https://cloud.google.com/load-balancing/docs/tutorials/optimize-app-latency>

Question: 26**CertyIQ**

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:**

Correct answers are (A) & (E)

Private Google Access interaction

<https://cloud.google.com/nat/docs/overview#interaction-pga>

Specifications

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

Question: 27**CertyIQ**

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:

Reference:

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

Question: 28

CertyIQ

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

Explanation:

Grant the read-only privilege to the service account for the Cloud Storage bucket.

Question: 29

CertyIQ

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

Explanation:

Correct Answer is (D):

All yaml files used by Deployment Manager as template used to resources provisioning, must be updated manually.

Question: 30**CertyIQ**

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**Explanation:**

GetIamPolicy and SetIamPolicy is only for service accounts. But question asks for a project members.

Hence, D and E are correct ans.

D - <https://cloud.google.com/iam/docs/granting-changing-revoking-access#granting-gcloud-manual>

E - <https://cloud.google.com/iam/docs/granting-changing-revoking-access#access-control-via-console>

Reference:

<https://cloud.google.com/iam/docs/granting-changing-revoking-access>

Question: 31**CertyIQ**

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:**

As the question states that the RTT is 100ms thus low transfer rate is due to the TCP window size that is too small. And the solution is to increase the window size .

Question: 32

CertyIQ

You work for a multinational enterprise that is moving to GCP.

These are the cloud requirements:

"Ç 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)

"Ç Multiple regional offices in Europe and APAC

"Ç Regional data processing is required in europe-west1 and australia-southeast1

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

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

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

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

Answer: A

Explanation:

Correct Answer is A

You cannot attach 2 NICs of same appliance to same VPC. The two NICs must be attached to different VPCs.

It cant be C or D because you need 2 VPCs.

<https://cloud.google.com/vpc/docs/create-use-multiple-interfaces>

Each interface is attached to a different VPC network, giving that instance access to different VPC networks in Google Cloud Platform (GCP). You cannot attach multiple network interfaces to the same VPC network.

It can't be B because you need to deploy the appliances in HOST Project to achieve CENTRALIZED NETWORK ADMINISTRATION

Question: 33

CertyIQ

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:

Correct Answer is A

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>

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)

Question: 34

CertyIQ

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

Explanation:

D be the answer.

"Globally distributed users report that their SMTP and IMAP services are slow" --> means it's needed to be global, traffic type is TCP.

"end-to-end encryption" + "you do not have access to the SSL certificates" ----> means that you can not use client certificate to configure on LB to do SSL offload.

As per the reference below, only TCP proxy Load Balancer.

<https://cloud.google.com/load-balancing/docs/choosing-load-balancer>

Question: 35

CertyIQ

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:

The correct answer is A & C

VPC peering offers peering between VPC which will suffice the requirement =AC is 100% correct

Question: 36

CertyIQ

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

Explanation:

Issue a cache invalidation command with pattern /folder-a/*.

Question: 37

CertyIQ

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

Explanation:

A. VPC flow logs

B. Firewall logs

Question: 38

CertyIQ

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

Explanation:

Correct Answer is D

Cloud Armour is applied at load balancers

Configuring Google Cloud Armor through Ingress.

<https://cloud.google.com/kubernetes-engine/docs/how-to/ingress-features>

Security policy features

Google Cloud Armor security policies have the following core features:

You can optionally use the QUIC protocol with load balancers that use Google Cloud Armor.

You can use Google Cloud Armor with external HTTP(S) load balancers that are in either Premium Tier or Standard Tier.

You can use security policies with GKE and the default Ingress controller.

Question: 39

CertyIQ

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

- A. Configure VPC peering in a full mesh.
- B. Alter the routing table to resolve the asymmetric route.

- C. Create network tags to allow connectivity between all three VPCs.
- D. Delete the legacy network and recreate it to allow transitive peering.

Answer: A

Explanation:

A is the right answer. VPC peering is not transitive. If you want any VPC to any VPC connection, you need to connect all VPCs in a full mesh manner.

Question: 40

CertyIQ

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:

Correct answer is D

"TFTP is a UDP-based protocol. Servers listen on port 69 for the initial client-to-server packet to establish the TFTP session, then use a port above 1023 for all further packets during that session. Clients use ports above 1023"

https://docstore.mik.ua/oreilly/networking_2ndEd/fire/ch17_02.htm

Besides, Google Cloud external TCP/UDP Network Load Balancing (after this referred to as Network Load Balancing) is a regional, non-proxied load balancer.

Network Load Balancing distributes traffic among virtual machine (VM) instances in the same region in a Virtual Private Cloud (VPC) network. A network load balancer directs TCP or UDP traffic across regional backends.

Question: 41

CertyIQ

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

Explanation:

VoIP uses SIP protocol which CAN use both TLS and UDP because of that the correct answer is B

<https://cloud.google.com/load-balancing/docs/choosing-load-balancer> External facing is internet facing . Looking at the flow chart via the url above and knowing VOIP are usually USP based, I would opt for external network loadbalancer

Question: 42

CertyIQ

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

Explanation:

It couldn't be A. Cause Cloud NAT is just an outbound NAT and can not DNAT the unsolicited incoming traffic from On-Prem to GCP. In order to intercept ,translate and forward an incoming session into GCP we need to provide additional DNAT rules on an intermediate GCP instance. So the answer will be C I guess.

Question: 43

CertyIQ

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

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

Answer: A

Explanation:

Correct Answer is (A)

Overview

By creating and managing SSH keys, you can let users access a Linux instance through third-party tools.

An SSH key consists of the following files:

A public SSH key file that is applied to instance-level metadata or project-wide metadata.

A private SSH key file that the user stores on their local devices.

If a user presents their private SSH key, they can use a third-party tool to connect to any instance that is configured with the matching public SSH key file, even if they aren't a member of your Google Cloud project.

Therefore, you can control which instances a user can access by changing the public SSH key metadata for one or more instances.

Reference:

<https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys>

Question: 44

CertyIQ

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

Explanation:

It is B Custom static routes can apply to all instances or specific instances. Static routes with a tag attribute apply to instances that have that same network tag. If the route doesn't have a network tag, the route applies to all instances in the network.

<https://cloud.google.com/vpc/docs/routes#subnet-routes>

Question: 45

CertyIQ

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:

When private cluster is activated, you can only access the master through dedicated IP ranges

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

Question: 46**CertyIQ**

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**Explanation:**

"B" be the correct answer

"For example, if your company has a security team that manages firewalls and SSL certificates and a networking team that manages the rest of the networking resources, then grant this role to the networking team's group."

Reference:

<https://cloud.google.com/compute/docs/access/iam>

Question: 47**CertyIQ**

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:**

Answer is C, well explained here https://cloud.google.com/load-balancing/docs/health-check-concepts#content-based_health_checks

Question: 48**CertyIQ**

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: B

Explanation:

compute.NetworkAdmin role contains compute.interconnectAttachments.* which is required for VLAN attachment deletions. None of the other options provide the permission so Answer B is correct.

Question: 49

CertyIQ

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

Explanation:

The correct answer is "D", see Canary Updates section from following link.

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

Question: 50

CertyIQ

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

Explanation:

A = Managed instance group and deployed in a set region (MIG is a regional resource) deployed in multiple zones

Question: 51

CertyIQ

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

Explanation:

Ans is D, Preventing caching Include a Cache-Control: private header in responses that should not be stored in Cloud CDN caches, or a Cache-Control: no-store header in responses that should not be stored in any cache, even a web browser's cache.

Question: 52

CertyIQ

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

What should you do?

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

Answer: A

Explanation:

A is correct, Cloud Armor whitelisting ensure only certain IP address can access the LB. deny all connection by default

Thank you

Thank you for being so interested in the premium exam material.
I'm glad to hear that you found it informative and helpful.

But Wait

I wanted to let you know that there is more content available in the full version.
The full paper contains additional sections and information that you may find helpful,
and I encourage you to download it to get a more comprehensive and detailed view of
all the subject matter.

[Download Full Version Now](#)



Future is Secured
100% Pass Guarantee



24/7 Customer Support
Mail us - certyiqofficial@gmail.com



Free Updates
Lifetime Free Updates!

Total: **172 Questions**

Link: <https://certyiq.com/papers?provider=google&exam=professional-cloud-network-engineer>