



- Expert Verified, Online, **Free**.

 Custom View Settings

Topic 1 - Single Topic

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.

🗨️ **kumarp6** 1 week, 1 day ago

Answer C.

upvoted 1 times

🗨️ **ZODOGAM** 3 months ago

The answer is C --- <https://cloud.google.com/load-balancing/docs/health-checks#fw-netlb>

upvoted 1 times

🗨️ **PeppaPig** 3 months, 3 weeks ago

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.

[https://cloud.google.com/load-balancing/docs/network/networklb-backend-service#firewall\\_rules](https://cloud.google.com/load-balancing/docs/network/networklb-backend-service#firewall_rules)

upvoted 2 times

🗨️ **PeppaPig** 3 months, 3 weeks ago

By pass-through, it means LB preserves the source IPs of incoming requests

upvoted 1 times

🗨️ **un** 7 months, 3 weeks ago

Answer is C

upvoted 1 times

🗨️ **EJJ** 8 months, 2 weeks ago

Answer is C. ref: [https://cloud.google.com/load-balancing/docs/https/setting-up-https#configuring\\_firewall\\_rules](https://cloud.google.com/load-balancing/docs/https/setting-up-https#configuring_firewall_rules)

upvoted 3 times

🗨️ **Vidyasagar** 9 months, 3 weeks ago

C is the one

upvoted 1 times

🗨️ **eeghai7thioyaiR4** 10 months, 2 weeks ago

Should we use cloud armor ?

Using firewall on the vm seems useless, because the customer will get through the load balancer, which is open

upvoted 3 times

🗨️ **nikiwi** 1 year ago

I passed the exam today, and a lot of questions were from this source. Google doesn't share the correctness percentage but I can share my personal answers to every question from this site if anyone is interested. Moving to Cloud Architect now :)

upvoted 3 times

🗨️ **Taufique** 3 months, 1 week ago

Please share your answer to me.

upvoted 1 times

🗨️ **network\_020** 7 months, 2 weeks ago

pls share the answers

upvoted 1 times

🗨️ **mwellger** 11 months ago

I would be interested in the answers you went with

upvoted 1 times

  **yas\_cloud** 11 months, 1 week ago

Hi - Can you please share your personal answers to questions from this site via email? Thanks

upvoted 1 times

  **[Removed]** 1 year, 1 month ago



Ans - C

upvoted 1 times

  **norwayping** 1 year, 1 month ago

C is the right one

upvoted 1 times

  **mlyu** 1 year, 2 months ago

Using Elimination



VPC service controls is not about application access control, so A n B is not correct.

Targeted label is not a valid target for firewall rule, see

[https://cloud.google.com/vpc/docs/firewalls#rule\\_assignment](https://cloud.google.com/vpc/docs/firewalls#rule_assignment)

So the only option C is correct answer

upvoted 1 times

  **EMO** 1 year, 3 months ago

Agreed, its C

upvoted 1 times

  **saurabh1805** 1 year, 4 months ago

C is correct answer

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

upvoted 1 times

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.

🗲️ 👤 **HateMicrosoft** Highly Voted 👍 1 year, 4 months ago

The correct answer is D. However the explanation is wrong.

We create one VPC network in auto mode that creates one subnet in each Google Cloud region automatically.

So, region us-east1 and europe-west1 are in the same network and they can communicate using their internal IP address even though they are in different Regions.

They take advantage of Google's global fiber network.

Creating an auto mode network

<https://cloud.google.com/vpc/docs/using-vpc#create-auto-network>

upvoted 8 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is D

upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 week, 6 days ago

Answer is D:

They will communicate over GCP's Private access Backbone...

upvoted 1 times

🗲️ 👤 **un** 7 months, 3 weeks ago

D is correct

upvoted 1 times

🗲️ 👤 **[Removed]** 9 months ago

internal communication is cheapest, VPC is global ,no need to go out of GCP

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D

upvoted 1 times

🗲️ 👤 **norwayping** 1 year, 1 month ago

D is the right one

upvoted 1 times

🗲️ 👤 **EMO** 1 year, 3 months ago

Agreed its D

upvoted 1 times

🗲️ 👤 **Capo** 1 year, 4 months ago

D is correct , its easier to configure and allow communication between the users,, if we use two vpc's then we need to add peering or other resources in order to allow communication among them, hence it will cost ur more as well and the design would not be considered as best practice

upvoted 1 times

🗲️ 👤 **saurabh1805** 1 year, 4 months ago

D is correct answer for me,

upvoted 1 times

🗲️ 👤 **Shaun\_Wang** 1 year, 7 months ago

Should be D, there is no networking peering since its a single VPC > I think the topic is talking about letting instances from 2 subnets to communicate to each other. However I do think its a bit confusing. Client needs to talk to the web tier through Global Load Balancer and use host and rules for forwarding to the specific instance group and communication between instance group should be within the same VPC.

upvoted 2 times

🗨️ 👤 **El\_Memer** 1 year, 10 months ago

Why is not C ? VPC Network Peering is for Connecting 2 VPC, in this case, the global load balancer normally fits right -->  
[https://cloud.google.com/load-balancing/docs/https/setting-up-https#cross-region\\_load\\_balancing](https://cloud.google.com/load-balancing/docs/https/setting-up-https#cross-region_load_balancing)

upvoted 1 times

🗨️ 👤 **KDMIndia** 8 months ago

And LB is not supported to sync backend workload. It's only LB for LB IP

upvoted 1 times

🗨️ 👤 **bimboom2** 1 year, 6 months ago

C Requires data leaving the google network which you will pay for. the reduce costs rules out c

upvoted 4 times

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.

🗲️ 👤 **Shaun\_Wang** Highly Voted 🍌 1 year, 7 months ago  
Definitely C.  
upvoted 12 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago  
Answer is C  
upvoted 1 times

🗲️ 👤 **yas\_cloud** 1 month, 1 week ago  
It would be C. D is also correct in terms of what mainly you want to achieve, but i believe it also incurs additional operational overhead.  
upvoted 1 times

🗲️ 👤 **lorca** 1 month, 1 week ago  
Selected Answer: C  
Definitely C.  
upvoted 1 times

🗲️ 👤 **B3nd3cida** 1 month, 2 weeks ago  
Best answer is C C.  
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.  
upvoted 1 times

🗲️ 👤 **Arad** 1 month, 3 weeks ago  
C is correct.  
upvoted 1 times

🗲️ 👤 **ThisisJohn** 2 months, 3 weeks ago  
I would say A, as it is written, does not guarantee isolation between for the third department, just simplifies operation through shared VPC. For me, the one which guarantees isolation is C  
upvoted 1 times

🗲️ 👤 **Vishaan** 7 months, 2 weeks ago  
Answer Should be A.  
Because its single Project with 3 Department. When you create 3 VPC it will be consider as 3 Projects. So C is the Wrong answer. With Shared VPC and IAM controls, you can separate network administration from project administration.  
upvoted 1 times

🗲️ 👤 **cloudy** 1 month, 3 weeks ago  
wrong, creating 3 VPCs won't be considered as creating 3 projects  
upvoted 2 times

🗲️ 👤 **un** 7 months, 3 weeks ago  
C is correct  
upvoted 1 times

🗲️ 👤 **EJJ** 8 months, 4 weeks ago  
Keyphrase/s:  
1. separate network administrative domains (can be achieved with seperate VPCs)  
2. reduce operational overhead (can be achieved using shared VPC)  
In order to fulfill the requirements: 2 VPCs connected to each other, 1 isolated VPC, and keyphrase no.1, the ANSWER is C. Keyphrase no.2 is just diversion.  
upvoted 3 times

🗨️ 👤 **Vidyasagar** 9 months, 3 weeks ago

C is the one  
upvoted 1 times

🗨️ 👤 **voyager** 11 months ago

The correct ans is "C". Shared VPC doesn't work with single project  
upvoted 2 times

🗨️ 👤 **voyager** 11 months ago

YES C.  
upvoted 1 times

🗨️ 👤 **narangikhatmal** 11 months, 4 weeks ago

C reason being seperate n/w domains.  
<https://cloud.google.com/vpc/docs/vpc-peering>  
upvoted 1 times

🗨️ 👤 **ydanno** 1 year ago

"A" is correct.  
The organization IS deployING a single project. The organization HAS NOT deploy a single project so we can change the project structure.  
Peered VPC networks remain administratively separate. They take a lot of operational overhead.  
We can implement a security best practice of least privilege for network administration and can operate less overhead using a Shared VPC network.  
upvoted 1 times

🗨️ 👤 **chetz12** 11 months, 3 weeks ago

The problem with option A is that it won't let you administer separate VPC/subnet as they are part of centralized VPC.  
C sounds the most reasonable if networks have to be managed in isolation  
upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C  
upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C  
upvoted 1 times

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`

🗲️ 👤 **rakeshvardan** Highly Voted 👍 1 year, 4 months ago  
It should be C only as suggested.

--zone-file-format  
Indicates that the input records-file is in BIND zone format. If omitted, indicates that the records-file is in YAML format.  
upvoted 7 times

🗲️ 👤 **saurabh1805** 1 year, 4 months ago  
yes you are right, correct answer should be C  
upvoted 2 times

🗲️ 👤 **kumarp6** Most Recent ⌵ 1 week, 1 day ago  
Answer is C  
upvoted 1 times

🗲️ 👤 **seddy** 8 months ago  
C  
-file format flag is necessary for BIND. If that flag is NOT used then the format would be YAML  
upvoted 1 times

🗲️ 👤 **EJJ** 8 months, 4 weeks ago  
ANS is C. --zone-file-format flag indicates that the input records-file is in BIND zone format. If omitted, indicates that the records-file is in YAML format. ref. <https://cloud.google.com/sdk/gcloud/reference/dns/record-sets/import>  
upvoted 2 times

🗲️ 👤 **[Removed]** 9 months ago  
--zone-file-format  
Indicates that the input records-file is in BIND zone format. If omitted, indicates that the records-file is in YAML format.  
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - C  
upvoted 1 times

🗲️ 👤 **norwayping** 1 year, 1 month ago  
C is the right one  
upvoted 1 times

🗲️ 👤 **saurabh1805** 1 year, 4 months ago  
D is correct option here, refer below link  
  
<https://cloud.google.com/sdk/gcloud/reference/dns/record-sets/import>  
upvoted 1 times

🗲️ 👤 **pelekafitinakwenu** 5 months, 1 week ago  
Why would you conclude D, when the link you have provided proves the answer is C, check the examples section, second command which is `gcloud dns record-sets import ZONE_FILE --zone-file-format --zone=MANAGED_ZONE`  
upvoted 1 times

🗲️ 👤 **paweu** 9 months, 1 week ago  
If you check this guy's link you will see C is right, click on --zone-file-format and you'll see bind format info.  
upvoted 2 times

🗲️ 👤 **saurabh1805** 1 year, 4 months ago  
C is correct answer  
upvoted 4 times



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.

  **jordi\_194** Highly Voted 1 year, 6 months ago

It has to be custom mode to avoid collision but in case of C 10.128.0.0/9 will collide with the ranges automatically created. 10.0.0.0/9 doesn't overlap with them.


<https://cloud.google.com/vpc/docs/vpc#ip-ranges>

upvoted 15 times

  **B3nd3cida** 1 month, 2 weeks ago

indeed!

upvoted 1 times

  **Pegpeng** 2 months, 2 weeks ago

you are right, I have test this in GCP, one VPC with auto mode, the other with custom, but with 10.128.0.0-9, there will be confliction.

upvoted 1 times

  **kumarp6** Most Recent 1 week, 1 day ago

Answer is B

upvoted 1 times



  **seddy** 8 months ago

It's B. You cannot peer an auto-mode VPC with another auto mode VPC since Google uses the same subnet CIDR range for all auto modes (10.128.0.0/9)

Thus Custom mode NW with a CIDR different from 10.128.0.0/9 is the necessary condition!

Peace :)

upvoted 1 times

  **Vidyasagar** 9 months, 3 weeks ago

B is the correct answer

upvoted 1 times

  **pentium2000** 9 months, 3 weeks ago

B, 200%

upvoted 2 times

  **voyager** 11 months ago

Ans B . 10.128.0.0/9 is used in auto mode creation and overlap

upvoted 2 times

  **[Removed]** 1 year, 1 month ago



Ans - B

upvoted 1 times

  **norwayping** 1 year, 1 month ago

B is the correct one

upvoted 1 times

  **EMO** 1 year, 3 months ago

B is the right answer

upvoted 1 times

  **ss\_1982** 1 year, 4 months ago



B is the right answer, other 3 options overlaps

upvoted 3 times

  **saurabh1805** 1 year, 4 months ago


B is correct answer, existing subnet can not be in range of C i.e. 10.128.0.0/9.  
<https://cloud.google.com/vpc/docs/vpc#subnet-ranges>

upvoted 4 times

  **dg63** 1 year, 6 months ago

"B" is appropriate answer

upvoted 4 times

  **serg3d** 1 year, 7 months ago

C range looks better

upvoted 1 times

  **ZODOGAM** 3 months ago

You only do it to sabotage the questions. serg3d

upvoted 1 times

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.

🗨️ 👤 **Ganshank** Highly Voted 👍 1 year, 8 months ago

A, D

Requires Private Google Access - <https://cloud.google.com/vpc/docs/private-access-options#pga>  
upvoted 23 times

🗨️ 👤 **buldas** 8 months, 4 weeks ago

Nope, as in <https://cloud.google.com/vpc/docs/configure-private-google-access>:

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.

This traffic will meet the firewal.

Should be C, as in <https://cloud.google.com/vpc/docs/configure-private-services-access>:

Private services access is a private connection between your VPC network and a network owned by Google or a third party. Google or the third party, entities who are offering services, are also known as service producers. The private connection enables VM instances in your VPC network and the services that you access to communicate exclusively by using internal IP addresses.

upvoted 2 times

🗨️ 👤 **catalinv** 7 months ago

Hi buldas, it can't be private service access, as this doesn't include Google services, but only 3rd party services, like Netapp.

upvoted 4 times

🗨️ 👤 **EJJ** Highly Voted 👍 8 months, 4 weeks ago

ANS is A,D.

Ref.:

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

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

"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."

upvoted 5 times

🗨️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is A & D

upvoted 1 times

🗨️ 👤 **desertlotus1211** 1 month, 1 week ago

The Answers are B & C: <https://cloud.google.com/vpc/docs/private-access-options>

Read the options carefully...

upvoted 1 times

🗨️ 👤 **desertlotus1211** 2 weeks, 1 day ago

Upon reviewing the question - the correct answers are A&E:

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

Under network configuration [which need to be satisfied for Google Private Access to work],under route options:

'Routing options

Your VPC network must have appropriate routes [default or custom] whose next hops are the default internet gateway.'

further down for configurations it shows you need to add a subnet... not VPC.

sorry about previous answer...

upvoted 1 times

  **JesusMariaJose** 1 month, 2 weeks ago

**Selected Answer: AD**

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>

upvoted 1 times

  **andrew\_9025** 1 month, 3 weeks ago

I think only A is correct in this case, It says choose 2 but no one of the others is a correct answer

A - turning on private google access allows the instances without a public ip to access a set of reserved internal ip addresses for managed services and establish the routes to reach those its automatically, and must be enabled on subnet level, so that would be enough to reach big query and pubsub

B - private google access is not enabled on VPC level, wrong answer

C - private services access is for used to establish peering toward google network services in their private network like the management plane of a Kubernetes cluster, and in general is used to reach services that comes in forms of a GCE instance like cloud SQL, and this is not the case

D,E - not would establish routes through the default internet gateway, but the question clearly states “without sending the traffic through the firewall”, so both are are wrong

upvoted 1 times

  **Arad** 1 month, 3 weeks ago

A & D are correct.

upvoted 1 times

  **retep007** 3 months, 3 weeks ago

A, D

C - Private service access doesn't support Pubsub and Bigquery

upvoted 2 times

  **PeppaPig** 4 months, 2 weeks ago



A&D 100%

Private Service Access is for different use cases where you need to access Google APIs via private endpoints that you define. To do that you need to create DNS records for your private endpoints, and assign internal IP addresses.

Traffic is routed through a custom route within your VPC, not through the internet gateway

<https://codelabs.developers.google.com/codelabs/cloudnet-psc#0>

upvoted 1 times

  **jeeet\_** 6 months, 1 week ago

Two name, Bigquery and pubsub are confusing.

A- makes sense as Google Private is activated at subnet level ( this makes option B out of league)

C- Private service is peering with other network, and accessing them via internal ips. (but bigquery and pubsub, they require none here).

D- makes no sense, as traffic will have to go via external IP (against the question).

E. Makes sense as traffic will never go out.

upvoted 1 times

  **catalinv** 7 months, 1 week ago

A - private google services - are customer's services in GCP. Check this video: [https://www.youtube.com/watch?v=wHvL\\_48ZhM8](https://www.youtube.com/watch?v=wHvL_48ZhM8) - I hope it clarifies it. And they are enabled at subnet level.

I am not sure about D or E, as the only difference is "external/internal IP addresses of Google APIs and services" - in the same video it says, internal VMs access to Google APIs are proxied to 199.36.153.4/30 subnet - these are public IPs, BUT - this subnet is not publicly routed. --> so is it external? or internal?

Thank you

upvoted 1 times

  **JohnnyBG** 5 months, 1 week ago

Google API respond to public IP so External

upvoted 1 times

  **Vishaan** 7 months, 2 weeks ago

Answer Should C,E. Bigquery and API is called Services.

Private services access is a private connection between your VPC network and a network owned by Google or a third party. Google or the third party, entities who are offering services, are also known as service producers. The private connection enables VM instances in your VPC network and the services that you access to communicate exclusively by using internal IP addresses. VM instances don't need Internet access or external IP addresses to reach services that are available through private services access

upvoted 1 times

🗨️ 👤 **seddy** 8 months ago

Normally both (A, D) and (C, E) work (no other combination can be the answer) But i would stick with (A, D) because I believe 'private services access' does not have access to Cloud Pub/Sub API but 'Private Google Access' does.

Peace :)

upvoted 1 times

🗨️ 👤 **qaz\_132** 3 months, 1 week ago

I will go with (A, D) as well, but just curious, where do you see " 'private services access' does not have access to Cloud Pub/Sub API"?

upvoted 1 times

🗨️ 👤 **Alex0303** 8 months, 3 weeks ago

I believe A, D - correct answer. A - obviously. D - 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. The source IP address of the packet can be the primary internal IP address of the network interface or an address in an alias IP range that is assigned to the interface. If you disable Private Google Access, the VM instances can no longer reach Google APIs and services; they can only send traffic within the VPC network.

upvoted 2 times

🗨️ 👤 **jdjorge** 8 months, 4 weeks ago

C and E. Private google access works only to Public IPs, Private Service Access works thru Internal IPs

<https://cloud.google.com/compute/docs/storing-retrieving-metadata>

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

upvoted 2 times

🗨️ 👤 **qaz\_132** 3 months, 1 week ago

What you said is wrong. The whole point of PGA is to allow VMs have internal IPs only to communicate with Google services. So, VMs do not need public IPs.

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

upvoted 1 times

🗨️ 👤 **jdjorge** 8 months, 4 weeks ago

C and E. Private google access works only to Public IPs, Private Google Access works thru Internal IPs

<https://cloud.google.com/compute/docs/storing-retrieving-metadata>

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

upvoted 1 times

🗨️ 👤 **Seven1** 9 months, 1 week ago

A is PSC at subnet level. But the docs say PGA is at VPC level. Thats B.

The PSA is also at VPC level for GCP VM instances.

VPC peering to an external IP address is the same as PSA, so C and D are basically the same thing.

I'd stick to B and either of C or D.

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

upvoted 1 times

🗨️ 👤 **qaz\_132** 3 months, 1 week ago

It is the opposite, PGA is at subnet level, PSC is at VPC level.

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

upvoted 1 times

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.

 **iloveme** Highly Voted 1 year, 3 months ago

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.

upvoted 11 times

 **kumarp6** Most Recent 1 week, 1 day ago

Answer is A

upvoted 1 times

 **andrew\_9025** 1 month, 3 weeks ago


the answer is B, the enable-oslogin set to false would prevent anyone to ssh into machines, anyway someone with the project owner role would still be able to it even though and that is the only case

A - would work only if you have a project owner role, else is wrong

B - correct, reset it, and then you can ssh if the machine is ready for that, meaning having ssh enabled with the keys in place

C,D wouldn't work, even if you are the project owner in this case, std ssh in unrelated from IAM roles, you simply can't ssh into machines due to the metadata enable-oslogin set to false


upvoted 1 times

 **desertlotus1211** 1 month, 3 weeks ago

Answer is A.... All other solutions require some sort of tampering with the GCP environment and/or project. The question asks to SSH into one instance - not all or some. Plus if you consider BPs - then you'd set OS-login to TRUE with 2FA. AND you need to configure IAM roles to grant or revoke SSH access to your instances... The answers don't reflect this nor the question. Too much effort just for one CE!

Answer should be A. Thoughts?

upvoted 1 times

 **ThisisJohn** 2 months, 3 weeks ago

I'd say it's B, as OS-login seems to be an alternative to SSH keys. The below is from this link <https://cloud.google.com/compute/docs/instances/managing-instance-access>

OS Login lets you use Compute Engine IAM roles to grant or revoke SSH access to your Linux instances. OS Login is an alternative to managing instance access by adding and removing SSH keys in metadata.

upvoted 1 times

 **aa\_desh** 4 months ago

A is worked, I have tested as below

- 1) Created VM
- 2) Set enable-oslogin FALSE ( in compute engine metadata) as well in VM's metadata
- 3) None of the instances are set with any SSH key, and no project-wide SSH keys have been configured (set block project wide ssh key on VM)
- 4) firewall allow for tcp:22
- 5) Try to ssh from cloud shell and web console, worked able to ssh into VM
- 5)

upvoted 4 times

 **Dia** 4 months, 1 week ago

D looks like the choice. as per <https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#addkey> : Instance-level public SSH keys: Use this metadata to give users special access—the ability to connect to a specific instance in your project—even if it blocks project-wide public SSH keys.

upvoted 1 times

 **PeppaPig** 4 months, 2 weeks ago

Using elimination

B is wrong. You still need ssh key pairs



C is wrong. Private key shall never expose to the outside  
D is wrong. Project-wide ssh keys is blocked

That leaves A is only correct answer  
upvoted 2 times

🗨️ 👤 **Zuy01** 4 months, 3 weeks ago

I think the best ans is A, cause i've tried to check "Block project-wide SSH keys" on particular instance on console and cannot connect to that instance.  
upvoted 2 times

🗨️ 👤 **okercho** 4 months, 3 weeks ago

I think A is the correct answer.

B: This would work, BUT, it also needs correct roles to be added to the user ([https://cloud.google.com/compute/docs/instances/managing-instance-access#configure\\_users](https://cloud.google.com/compute/docs/instances/managing-instance-access#configure_users)), and that part is not done nor mentioned.

C: Private key is not the one added into metadata. This doesn't make any sense, thus, is wrong.

D: This would work, BUT statement says "ALL instances in project are configured to block project-wide SSH keys", thus, as we're adding the key to the project metadata, this won't work.

I've also tested A in sandbox project and works perfectly.  
upvoted 2 times

🗨️ 👤 **JoeShmoe** 7 months, 2 weeks ago

I think its A. The key inference here is you want to access one instance temporarily and we are assuming you are a gcloud or console user with instance admin permissions. Using cloud shell or cloud ssh a temporary private key is generated on-demand and held in the browser. The corresponding public key is created and added to project wide or instance specific metadata. The public key has additional information associated with it, including an expiry timestamp, which renders it invalid after a few minutes. The public key is set on the project's metadata unless the instance to which you're connecting via SSH has the "block project wide SSH keys" attribute set; in that case, the public key is set on the instance's metadata.

D is wrong as you would allow access to all instances. C would work but it requires the user to manage the key pairs

4. When you SSH using the gcloud tool (for example, `gcloud compute ssh`) [4], you have to be authenticated to the gcloud tool as a compute instance admin  
upvoted 3 times

🗨️ 👤 **[Removed]** 9 months ago

I support A, it is a standard recommend why GCP chose  
upvoted 1 times

🗨️ 👤 **ude** 9 months ago

Not C and D, as "Adding SSH keys to a user account" , not Project or instace [https://cloud.google.com/compute/docs/instances/ssh#third-party-tools\\_1](https://cloud.google.com/compute/docs/instances/ssh#third-party-tools_1)  
upvoted 1 times

🗨️ 👤 **CloudTrip** 9 months, 2 weeks ago

Read the question again project wide access and metadata setting with FALSE is already enabled that makes B, D is absolutely wrong choice here. A also is a wrong choice as individual instance ssh is not enabled. So for a specific instance C is the right answer. Those who have practically used it will know how it works through putty to connect at OS level.  
upvoted 2 times

🗨️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is the one  
upvoted 2 times

🗨️ 👤 **eeghai7thioyaiR4** 10 months, 2 weeks ago

I believe this is A: connect using `gcloud compute ssh`

I just made some tests : I have a newly created google account, I never set any ssh keys in it anyhow

I create a VM, using default settings etc

At this point, none of the SSH keys that lives on my PC are actually deployed inside that VM

Yet I can connect via `gcloud compute ssh`, because an SSH keys and an account is preinstalled

Also, when you think about it .. it is actually the simplest solution, perhaps too obvious to be true  
upvoted 3 times

🗨️ 👤 **sc00by** 9 months, 2 weeks ago

works perfectly.

```
student_02_5f2889xxxx@cloudshell:~ (qwiklabs-gcp-02-4b88xxx753)$ gcloud compute ssh instance-3 --zone=us-central1-a
Updating instance ssh metadata...::Updated [https://www.googleapis.com/compute/v1/projects/qwiklabs-gcp-02-4b884eb49753/zones/us-central1-a/instances/instance-3].
Updating instance ssh metadata...done.
Waiting for SSH key to propagate.
Warning: Permanently added 'compute.3801805569292323095' (ECDSA) to the list of known hosts.
```

Linux instance-3 4.19.0-14-cloud-amd64 #1 SMP Debian 4.19.171-2 (2021-01-30) x86\_64

The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.


Last login: Sat Apr 3 23:20:21 2021 from 74.125.77.98

upvoted 1 times

  **looseboy** 10 months, 3 weeks ago

I agree with "A"

upvoted 1 times

  **looseboy** 10 months, 3 weeks ago

Sorry, B is correct

upvoted 1 times



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.

 **Ganshank** Highly Voted 1 year, 8 months ago

A


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

upvoted 10 times

 **kumarp6** Most Recent 1 week, 1 day ago

Answer is A

upvoted 1 times

 **desertlotus1211** 1 week, 6 days ago

Answer is A:

<https://cloud.google.com/network-connectivity/docs/interconnect/concepts/best-practices>

Configure VLAN attachments in the Shared VPC host project

'In a Shared VPC network, configure all VLAN attachments, not physical Interconnect connections (ports), in the host project. For more information about connecting attachments to Shared VPC networks'...

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

'You must create VLAN attachments and Cloud Routers for an Interconnect connection only in the Shared VPC host project'

upvoted 1 times

 **[Removed]** 1 year, 1 month ago

Ans - A

upvoted 1 times

 **ESP\_SAP** 1 year, 2 months ago

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

upvoted 3 times

 **ravirajani** 1 year, 4 months ago

B is correct Ans

In A, you create VLAN attachment in hostproject which has shared VPN and On-prem Interconnect. Than how departments will connect to Interconnect from their projects?

B is correct approach. VLAN attachments are created in service projects of individual departments. It uses "In another project" option to define where is Interconnect.

upvoted 1 times

🗨️ 👤 **ravirajani** 1 year, 3 months ago

A is right ans.

Service projects can't create VLAN attachments.

upvoted 1 times

🗨️ 👤 **saaurabh1805** 1 year, 4 months ago

A is correct answer and also recommended Google solution.

upvoted 1 times

🗨️ 👤 **HateMicrosoft** 1 year, 4 months ago

The correct answer is A

Shared VPC overview

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

upvoted 2 times

🗨️ 👤 **dxloader** 1 year, 6 months ago

A is correct

upvoted 1 times

🗨️ 👤 **elguije** 1 year, 7 months ago

I think A is the right answer.

When using a Shared VPC Network with Dedicated Interconnect, consider the following:

VLAN attachments and Cloud Routers for Dedicated Interconnect must exist in the Shared VPC host project, not in any service projects attached to the host project. When you create the Cloud Router to manage a VLAN attachment, you specify a particular VPC network. Effectively, the combination of a VLAN attachment and its associated Cloud Router are unique to a given Shared VPC network.

Service Project Admins can create VMs that use subnets in a Shared VPC network of a host project based on the permissions they have to the host project. VMs that use the Shared VPC network can use the custom dynamic routes for VLAN attachments available to that network.

upvoted 2 times

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

🗲️ 👤 **HateMicrosoft** Highly Voted 👍 1 year, 4 months ago

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

Session affinity options

[https://cloud.google.com/load-balancing/docs/internal#session\\_affinity](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.

upvoted 14 times

🗲️ 👤 **kumarp6** Most Recent ⌵ 1 week, 1 day ago

Answer is B

upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 month, 1 week ago

Answer is B: <https://medium.com/google-cloud/google-cloud-load-balancer-setup-tweaking-and-observations-c12d704e6d52>'

ffinity

Typically the LB is going to route new requests to any instance and traffic from one connection is going to route to the same instance. Say you want to set stickiness to make sure all connections from one client go to the same instance. Configure session affinity to client IP. You can also set by cookie. The GCLB sends a cookie on the first client request and future incoming requests with that cookie will be sent to the same instance.

upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 month, 3 weeks ago

Is the answers showing the syntax to use?

upvoted 1 times

🗲️ 👤 **EJJ** 8 months, 4 weeks ago

ANS is B. HTTP traffic uses TCP, TFTP uses UDP. Session Affinity does not work in UDP traffic, thus, using protocol and port is useless.

Ref:<https://cloud.google.com/load-balancing/docs/internal>

"Session affinity works on a best-effort basis for TCP traffic. Because the UDP protocol doesn't support sessions, session affinity doesn't affect UDP traffic."

upvoted 2 times

🗲️ 👤 **CloudTrip** 9 months, 2 weeks ago

Question mentions about HTTPS i.e. TCP and TFTP i.e. UDP protocols in an internal load balancer so it's definitely provides Client IP, Protocol and IP as options. So answer D is correct. [https://cloud.google.com/load-balancing/docs/backend-service#session\\_affinity](https://cloud.google.com/load-balancing/docs/backend-service#session_affinity)

upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 month, 3 weeks ago

D shows: Client IP, port and protocol... only 3 out of 4. Where is the Destination IP? this also looks like c as well BUT without the comma...

upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 month, 3 weeks ago

If it was showing all 4 wouldn't look like: Client, IP, port and protocol? With 2 commas separating?

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

B is the one

upvoted 1 times

🗨️ 👤 **HHHHHHH** 10 months, 3 weeks ago  
Why not D, TFTP is UDP protocol  
upvoted 1 times

🗨️ 👤 **nikiwi** 1 year, 1 month ago  
why not D?  
The same client could be accessing both HTTP and FTP, so the session stickiness based on Client IP only is not enough.  
upvoted 1 times

🗨️ 👤 **nikiwi** 1 year, 1 month ago  
on one more read, it is still ONE application that handles both services, so the Client IP is fine in that case.  
upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - B  
upvoted 1 times

🗨️ 👤 **passtest100** 1 year, 4 months ago  
should be D. the less metrics you choose, the lworse load balance among the instances.  
for example, for B, it is true that the session keep to the same instance, but it is always kept to the SAME instance only if the same source ip and destination ip for the both protocols  
upvoted 2 times

🗨️ 👤 **runtheworld** 1 year, 4 months ago  
Answer B  
2-tuple hashing, which uses the source and destination IPs. All connections from a client will end up on the same instance regardless of protocol as long as the instance stays healthy.  
  
<https://cloud.google.com/load-balancing/docs/target-pools#sessionaffinity>  
upvoted 1 times

🗨️ 👤 **beebie** 1 year, 5 months ago  
How can it be D when it says sticky across both the services?  
upvoted 2 times

🗨️ 👤 **knoor** 1 year, 5 months ago  
same question in ACG, recommends "D"  
upvoted 1 times

🗨️ 👤 **Barry123456** 1 year, 6 months ago  
clients are sticky to a particular instance across both services.  
  
"across both services"  
  
It's A, client IP only.  
upvoted 1 times

🗨️ 👤 **Barry123456** 1 year, 6 months ago  
er B. need an edit buton!  
upvoted 1 times

🗨️ 👤 **jordi\_194** 1 year, 6 months ago  
I'm a bit in doubt as in the subject it says internal application and Internal TCP/UDP LB supports all 3 options so I think it could be also C.  
[https://cloud.google.com/load-balancing/docs/backend-service#session\\_affinity](https://cloud.google.com/load-balancing/docs/backend-service#session_affinity)  
[https://cloud.google.com/load-balancing/docs/internal#session\\_affinity](https://cloud.google.com/load-balancing/docs/internal#session_affinity)  
[https://cloud.google.com/load-balancing/docs/https#session\\_affinity](https://cloud.google.com/load-balancing/docs/https#session_affinity)  
upvoted 1 times

🗨️ 👤 **Jos** 1 year, 6 months ago  
In that case one customer's HTTP session could go to a backend server and the TFTP flow to a different one. To have all sessions from one customer tied to an specific backend server i would be agree with "Client IP" answer.  
upvoted 3 times

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.

  **elguije** Highly Voted 1 year, 7 months ago

I think correct answer should be D.

<https://cloud.google.com/blog/products/identity-security/google-cloud-firewall-rules-logging-how-and-why-you-should-use-it>

"Since we have implicit ingress and the denial rule is not being logged, we create a “deny all” rule with priority 65534 to capture anything that gets denied"



<https://cloud.google.com/vpc/docs/firewall-rules-logging>

upvoted 15 times

  **kumarp6** Most Recent 1 week, 1 day ago

Answer is D

upvoted 1 times

  **desertlotus1211** 1 week, 6 days ago

Answer is D:



Implicit FW rule [ingress or egress] are NOT logged...

upvoted 1 times

  **Arad** 1 month, 3 weeks ago

D is correct.

upvoted 1 times

  **jeeet\_** 6 months, 3 weeks ago

Initially I chose A. (Wrong).

Correct is D.

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

Ingress packets are sampled after ingress firewall rules. If an ingress firewall rule denies inbound packets, those packets are not sampled by VPC Flow Logs.

--> it says, if an ingress firewall rule denies something, that won't be logged in VPC flow logs. That makes Option A out and wrong.

for sake of explanation-->

Egress packets are sampled before egress firewall rules. Even if an egress firewall rule denies outbound packets, those packets can be sampled by VPC Flow Logs.

which means--> creating

Option B and C -> makes no sense, as question talks about RDP.

Option D -> by default without explanation is the answer.

as you cannot monitor implied deny rules, you create a custom one to monitor. makes more sense.



upvoted 1 times

  **qch2012** 9 months, 2 weeks ago

D is incorrect because of the priority setting 65500, the implicit deny has lowest priority 65535, if you create a deny all rule in 65500, it would have impact on other rules with priority between 65500 - 65534.

A is correct in this case . For ingress traffic, VPC flow logs works after firewall rule , since firewall rule only allow HTTP traffic, it means the rest blocked traffic will be sampled by VPC flow log

upvoted 1 times

  **sc00by** 8 months, 3 weeks ago



you cannot inspect traffic with VPC flow because:



Ingress packets are sampled after ingress firewall rules. If an ingress firewall rule denies inbound packets, those packets are not sampled by VPC Flow Logs.



upvoted 2 times



  **Vidyasagar** 9 months, 3 weeks ago



D is correct  
upvoted 1 times



  **looseboy** 10 months, 1 week ago  
Ans is D.  
You cannot enable Firewall Rules Logging for the implied deny ingress and implied allow egress rules.  
upvoted 2 times



  **JoeShmoe** 7 months, 3 weeks ago  
this is exactly why D is correct  
upvoted 1 times



  **JoeShmoe** 7 months, 3 weeks ago  
The implicit rules have the lowest possible priority (65535)  
upvoted 1 times



  **voyager** 10 months, 2 weeks ago  
Definitely A - Implied rules deny all in engress with some exceptions: local traffic, ssh, rdp and icmp protocol. The firewall doesn't block RDP packtes in engress.  
upvoted 1 times



  **ydanno** 1 year ago  
Definitely "D" is correct.  
Ingress packets in VPC Flow Logs are sampled after ingress firewall rules.  
If an ingress firewall rule denies inbound packets, those packets are not sampled by VPC Flow Logs.  
We want to see the logs for blocked traffic so we have to look for them in firewall logs.  
[https://cloud.google.com/vpc/docs/flow-logs#key\\_properties](https://cloud.google.com/vpc/docs/flow-logs#key_properties)  
upvoted 1 times



  **[Removed]** 1 year, 1 month ago  
Ans - D  
upvoted 1 times

  **ESP\_SAP** 1 year, 2 months ago  
Correct Answer is (A):  
  
Using VPC Flow Logs  
VPC Flow Logs records a sample of network flows sent from and received by VM instances, including instances used as GKE nodes. These logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization.  
  
This page assumes you are familiar with the concepts described in VPC Flow Logs overview.  
  
Enabling VPC flow logging  
When you enable VPC Flow Logs, you enable for all VMs in a subnet. However, you can cut down the amount of information written to logging. Refer to Log sampling and aggregation for details on the parameters you can control.  
  
<https://cloud.google.com/vpc/docs/using-flow-logs>  
upvoted 3 times

  **EMO** 1 year, 3 months ago  
Correct Ans is D , We have to log in firewall <https://cloud.google.com/vpc/docs/firewall-rules-logging>  
upvoted 1 times

  **HateMicrosoft** 1 year, 4 months ago  
The correct anwser is D  
  
Unlike VPC flow logs, firewall rules logs are not sampled.Every connection is logged.  
  
Enabling firewall rules logging  
<https://cloud.google.com/vpc/docs/using-firewall-rules-logging#enable>  
upvoted 1 times

  **dxloader** 1 year, 6 months ago  
D is correct  
upvoted 2 times

  **architect** 1 year, 6 months ago  
Definitely D - this question is about firewall logging.  
upvoted 2 times

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.

🗲️ 👤 **ss\_1982** Highly Voted 👍 1 year, 4 months ago

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.

upvoted 10 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is A

upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 month, 2 weeks ago

Answer is A: [https://cloud.google.com/vpc/docs/shared-vpc#net\\_and\\_security\\_admins](https://cloud.google.com/vpc/docs/shared-vpc#net_and_security_admins)

it's states: 'A Shared VPC Admin can define a Security Admin by granting an IAM principal the Security Admin (compute.securityAdmin) role to the host project. Security Admins manage firewall rules and SSL certificates.'

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - A

upvoted 1 times

🗲️ 👤 **beebie** 1 year, 5 months ago

Should be A

upvoted 1 times

🗲️ 👤 **dg63** 1 year, 6 months ago

"A" - based on least privilege approach

upvoted 3 times

🗲️ 👤 **Darius\_Th3D0G** 1 year, 5 months ago

Yes, it's A.

[https://cloud.google.com/vpc/docs/shared-vpc#net\\_and\\_security\\_admins](https://cloud.google.com/vpc/docs/shared-vpc#net_and_security_admins)

upvoted 2 times

🗲️ 👤 **Supernhi** 1 year, 6 months ago

<https://cloud.google.com/vpc/docs/shared-vpc> . It's B

upvoted 2 times

🗲️ 👤 **desertlotus1211** 1 month, 2 weeks ago

Service Project Admins are only given the ability to create and manage instances that make use of the Shared VPC network

upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 month, 2 weeks ago

Answer is not B....

upvoted 1 times

🗲️ 👤 **Jos** 1 year, 6 months ago

A "shared VPC admin", not clear what that could be :), cannot give that kind of permissions. It's D for me.

upvoted 2 times



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.

🗳️ 👤 **kumarp6** 1 week, 1 day ago

Answer is C

upvoted 1 times

🗳️ 👤 **Arad** 1 month, 3 weeks ago

C is correct.

upvoted 2 times

🗳️ 👤 **ThisisJohn** 1 month, 3 weeks ago

Why not just creating the instance?

You can configure external IPv6 addresses on virtual machine instances (VMs) if the subnet that they are connected to has external IPv6 addresses enabled. Enabling external IPv6 addresses on a subnet is supported in some regions.

Ref <https://cloud.google.com/compute/docs/ip-addresses/configure-ipv6-address>

upvoted 2 times

🗳️ 👤 **jeeet\_** 6 months, 1 week ago

Answer is C,

B- Why Not?

just try to create a TCP LB, with default settings, you'll not get option to select IPV6,

But if you chose Global LB, then you'll get the option.

Concept- you're LB should be GLOBAL in order to have IPV6 IP Address. So read option C again.

upvoted 2 times

🗳️ 👤 **pythonrocks** 6 months ago

A global LB can be: HTTP(S), SSL proxy, tcp proxy. So the B is better than C as it is more accurate.

upvoted 1 times

🗳️ 👤 **pentium2000** 9 months, 2 weeks ago

C, there are LBs which support Global ipv4/ipv6

HTTP(S)

SSL Proxy

TCP Proxy

upvoted 1 times

🗳️ 👤 **Vidyasagar** 9 months, 3 weeks ago

C is correct

upvoted 1 times

🗳️ 👤 **narangikhatmal** 1 year ago

if you refer this page <https://cloud.google.com/load-balancing/docs/choosing-load-balancer>.

TCP proxy is listed as global so its implied as global TCP proxy. Ans i B.

upvoted 2 times

🗳️ 👤 **Ocedoc** 11 months, 2 weeks ago

I agree. If you instructed someone to execute C, they would more specifically execute B.

upvoted 1 times

🗳️ 👤 **Ocedoc** 11 months, 2 weeks ago

Upon review, I agree with rezavage., at premium tier, https and ssl proxy LBs also offer global LB. Changing to (C) since (B) is unnecessarily specific.

upvoted 1 times

🗳️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C



upvoted 1 times

🗳️ 👤 **EMO** 1 year, 3 months ago



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.

upvoted 2 times

  **DCW1** 1 year, 3 months ago

B, just follow the decision tree:

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

upvoted 1 times

  **rezavage** 1 year, 3 months ago

Note that it requires to be global. TCP load balancer could be regional or global. B is not a precise solution.



upvoted 1 times

  **saurabh1805** 1 year, 4 months ago

C should be correct answer, Gloabal Load Balancer (https) is one of load balancer supports Ipv6 address.


<https://cloud.google.com/load-balancing/docs/ipv6>

upvoted 3 times

  **beebee** 1 year, 5 months ago

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

upvoted 1 times

  **beebee** 1 year, 5 months ago

Should be C

upvoted 3 times

  **maxth3mad** 1 year, 5 months ago

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

"B"

upvoted 2 times

  **rezavage** 1 year, 3 months ago

TCP Proxy load balancer could be an option but it supports IPv6 only if it is implemented in global type which requires premium tier. the same goes for Https and SSL proxy load balancer . they all should be Global not Regional in order to support IPv6.so the answer will be C.

upvoted 5 times

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. "ç Create a Cloud VPN instance. "ç Create a policy-based VPN tunnel per subnet. "ç Configure the appropriate local and remote traffic selectors to match your local and remote networks. "ç Create the appropriate static routes.
- B. "ç Create a Cloud VPN instance. "ç Create a policy-based VPN tunnel. "ç Configure the appropriate local and remote traffic selectors to match your local and remote networks. "ç Configure the appropriate static routes.
- C. "ç Create a Cloud VPN instance. "ç Create a route-based VPN tunnel. "ç Configure the appropriate local and remote traffic selectors to match your local and remote networks. "ç Configure the appropriate static routes.
- D. "ç Create a Cloud VPN instance. "ç Create a route-based VPN tunnel. "ç Configure the appropriate local and remote traffic selectors to 0.0.0.0/0. "ç Configure the appropriate static routes.

🗲️ 👤 **Windows98** Highly Voted 👍 1 year, 2 months ago

D - Because you can't update the selectors after creating the VPN they need to be left open.

This from GCP:

When you create a route based tunnel using the Cloud Console, Classic VPN performs both of the following tasks:

Sets the tunnel's local and remote traffic selectors to any IP address (0.0.0.0/0)

For each range in Remote network IP ranges, Google Cloud creates a custom static route whose destination (prefix) is the range's CIDR, and whose next hop is the tunnel.

upvoted 9 times

🗲️ 👤 **sizzlelee** Highly Voted 👍 1 year, 3 months ago

with route-based, you dont have to select local networks, only remote networks.. Answer should be B

upvoted 6 times

🗲️ 👤 **Loved** 2 months, 3 weeks ago

But the device support only IKEv2... and with IKEv2 is not possible to use policy-based

upvoted 1 times

🗲️ 👤 **sc00by** 9 months, 2 weeks ago

Option D is better, because everytime you add a new remote network you have to delete and recreate the tunnel again adding up the new remote network.

With option D you do not have to recreate the tunnel.

upvoted 3 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is D

upvoted 1 times

🗲️ 👤 **giovane86** 1 month, 1 week ago

**Selected Answer: D**

ans - D

upvoted 1 times

🗲️ 👤 **seddy** 8 months, 1 week ago

I think the answer is B by elimination. It cannot be C or D because in route-based VPN, we only specify the remote ranges (namely, right side configuration). We DO NOT specify the local (left side) ranges. This is a trick question. Under normal circumstances, I would prefer route-based, but the question tests your knowledge on whether you know how to configure a route-based tunnel.

upvoted 1 times

🗲️ 👤 **[Removed]** 8 months, 4 weeks ago

Choosing between B and D, [https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#creating\\_a\\_gateway\\_and\\_tunnel](https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#creating_a_gateway_and_tunnel). Policy based cost 3 steps. Rule-based cause 2 steps.

upvoted 1 times

🗲️ 👤 **WakandaF** 9 months ago

What's the best answer?

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D the one

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Err - Should be D

upvoted 1 times

🗨️ 👤 **pizdecvsemu** 1 year, 3 months ago

Looks like D for me.

We have 2 tasks here - traffic selection and routing.

To avoid tunnel re-creation for new networks we can use 0.0.0.0/0 as traffic selector and Cloud VPN supports it for route- and policy-based VPNs.

For routing - create routes that are more specific than the traffic selector.

Another point - A best practice is to use 30 or fewer CIDRs per traffic selector. We want "summary" for traffic selection, and 0/0 is the best.

upvoted 4 times

🗨️ 👤 **Rodine** 10 months, 2 weeks ago

The remote traffic selector defines the set of remote IP ranges (CIDR blocks) from the perspective of the VPN gateway that emits the VPN tunnel. For Cloud VPN tunnels, the remote traffic selector is the right side or peer network.

B is the answer.

upvoted 1 times

🗨️ 👤 **Rodine** 10 months, 2 weeks ago

I mean that.

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.

upvoted 2 times

🗨️ 👤 **ravirajani** 1 year, 4 months ago

When Network Grows, I have to go back and add routes in Option B, which violates question constraint.

With Option D, i don't have to rework on routes, when new network subnets are added in VPC.

upvoted 5 times

🗨️ 👤 **ravirajani** 1 year, 3 months ago

[https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#routing\\_option\\_differences](https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#routing_option_differences)

Important: Traffic selectors cannot be changed after a tunnel has been created. If traffic selectors need to be changed in the future, you must delete and re-create the tunnel.

upvoted 3 times

🗨️ 👤 **rezavage** 1 year, 3 months ago

The answer is D, but just as a reminder I should say that traffic selector has nothing to do with routes. Traffic selector states that which traffics should be tunneled and for the route-based VPN it is always any traffic (0.0.0.0/0), whereas for the policy-based we explicitly define by the traffic selector. and as the question wanted the solution is future proof the solution should be route-based.

upvoted 4 times

🗨️ 👤 **Sheeda** 1 year, 4 months ago

B is correct, yes

upvoted 2 times

🗨️ 👤 **saurabh1805** 1 year, 4 months ago

B seems to b correct answer. refer below link

[https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#creating\\_a\\_gateway\\_and\\_tunnel](https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns#creating_a_gateway_and_tunnel)

upvoted 2 times

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.

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

"ç 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.

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

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

"ç 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.

🗲️ 👤 **BobBui** Highly Voted 👍 10 months, 1 week ago

I go with B&C, <https://cloud.google.com/dns/docs/best-practices>  
upvoted 9 times

🗲️ 👤 **sc00by** 9 months, 2 weeks ago

Indeed, because they are using custom DNS, on the other hand Cloud DNS cannot manage interorganizations DNS queries.  
upvoted 1 times

🗲️ 👤 **JohnnyBG** 6 months ago

It cannot be B, therefore ans is C&D  
[https://cloud.google.com/dns/docs/best-practices#best\\_practices\\_for\\_dns\\_forwarding\\_zones\\_and\\_server\\_policies](https://cloud.google.com/dns/docs/best-practices#best_practices_for_dns_forwarding_zones_and_server_policies)

Note: DNS forwarding cannot be used to forward between different Google Cloud environments, regardless of which way they are interconnected. For that use case, use DNS peering.  
upvoted 1 times

🗲️ 👤 **Bill831231** 2 months ago

just wondering, why there is no option for vpc peering  
upvoted 1 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : B and C  
upvoted 1 times

🗲️ 👤 **buldas** 9 months ago

I would say its B and C,  
C is quite obvious

And B because both orgs having they own DNS resolutions, so it's easier to make just DNS forwarding.  
upvoted 1 times

🗲️ 👤 **densnoigaskogen** 7 months ago

























DNS forwarding can not be used to forward between different Google Cloud environments, regardless of which way they are interconnected. For that use case, use DNS peering.  
This is noted in <https://cloud.google.com/dns/docs/best-practices>, thus, B should not be correct.  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

C and D  
upvoted 2 times

🗲️ 👤 **groovyygorilla** 1 year ago

I agree with B&C  
upvoted 2 times

-   **nikiwi** 1 year, 1 month ago  
I'd chose B,C  
It is the quickest and negligible downtime.  
upvoted 4 times
-   **Hybrid\_Cloud\_boy** 1 year, 1 month ago  
Hey D and not B? Downtime?  
upvoted 1 times
-   **[Removed]** 1 year, 1 month ago  
Ans - CD  
upvoted 1 times
-   **lukedj87** 1 year, 2 months ago  
Vote for B&D.  
DNS forwarding is used because it's mentioned they implement a CUSTOM DNS solution (otherwise you would use DNS peering...)  
VPN is the only reasonable thing I find. I would probably use anyway VPC peering if it was an option.  
upvoted 1 times
-   **2cool2touch** 1 year, 3 months ago  
D cannot be the answer. you cannot create A records for a zone you dont host. So each org can/should only create A record for its own records only.  
  
B&C are the quickest and minimal downtime solutions  
upvoted 1 times
-   **rezavage** 1 year, 3 months ago  
B and C will be the answer. If it says Cloud DNS I would go with D since zone transfer is unavailable. But base on the current situation both organizations have customized DNS and that means you may have both DNS use Forwarders and zone transfers in order to be able cross organization name resolution.  
upvoted 4 times
-   **pizdecvsemu** 1 year, 3 months ago  
C&D  
Cloud Interconnect is not for GCP-to-GCP;  
They already use Shared VPC, no IP conflicts - VPN terminated in Host projects is the way to go.  
upvoted 1 times
-   **[Removed]** 1 year, 4 months ago  
I guess answer will be B and D, because the organisations are already in Shared VPC modes, so no need for VPC peering or interconnect. You need DNS forwarding to resolve the names of other VPC so B and then you need to assign IP for VM so that it can be resolved from other VM  
upvoted 2 times
-   **HateMicrosoft** 1 year, 4 months ago  
The correct answer is C&D.  
  
Supported networks  
<https://cloud.google.com/network-connectivity/docs/vpn/concepts/choosing-networks-routing>  
upvoted 1 times
-   **COOL2020** 1 year, 5 months ago  
Definity C&D  
upvoted 3 times
-   **terrain** 1 year, 5 months ago  
Based on the requirement that they want to connect VPCs as quick as possible and with minimal downtime, I would say the correct answers are C & D. There is no requirement to consider Cloud Interconnect so A should be wrong.  
upvoted 2 times
-   **dxloader** 1 year, 6 months ago  
How to provision cloud interconnect to connect both organizations together?  
Isn't cloud interconnect used for connecting cloud with on-prems?  
Why C is wrong?  
upvoted 2 times

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.

  **glk** Highly Voted 1 year ago

Answer is D:  
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>

upvoted 9 times

  **Windows98** Highly Voted 1 year, 2 months ago



D - GCP doesn't run ECMP across different ASNs

upvoted 7 times

  **kumarp6** Most Recent 1 week, 1 day ago

Answer is : D

upvoted 1 times

  **Vidyasagar** 9 months, 3 weeks ago

D is right

upvoted 1 times

  **groovygorilla** 1 year ago

Agree with glk, answer is D. This reference says it all:  
<https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting#ecmp>

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

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Ans - D



upvoted 1 times

  **genesis3k** 1 year, 2 months ago

Correct answer is D. Please refer below:  
"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."

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

upvoted 3 times

  **Aniyadu** 1 year, 3 months ago

The answer seems to be D. As per standard practices we can only one ASN configured in on-premise.

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

upvoted 1 times



 **passtest100** 1 year, 4 months ago

change to A. The BGP session is established. so B is wrong. BGP(EBGP and IBGP) by default has only one optimal route in routing table. So whether ASN is the same or different, the issue still exists. Only if the routes are different, routes of the two routers will be in the routing table.

upvoted 1 times

  **passtest100** 1 year, 4 months ago

sorry, typo. it should be B is the possible answer.

upvoted 1 times

  **passtest100** 1 year, 4 months ago

should be C. no information in the question shows two ASNs is wrong. it should be reasonable that one data center can have multiple ASNs, since ASN has nothing to do with geo location. The two ASNs work well in the data center, as supposed in the question, the question is why the VPN with one of the routers cannot be setup. so C is the only possible answer.

upvoted 1 times

  **HateMicrosoft** 1 year, 4 months ago

The correct answer is D.

autonomous system number (ASN)

An autonomous system number (ASN) is a unique identifier that is globally available and allows its autonomous system to exchange routing information with other systems

An autonomous system (AS) is a group of IP prefixes with a clearly defined external routing policy. In order for multiple autonomous systems to interact, each needs to have a unique identifier.

So, one of these on-premises routers has this autonomous system number (ASN) wrongly done.

upvoted 3 times

  **COOL2020** 1 year, 5 months ago

D is the correct answer :)

upvoted 2 times

  **sagitarious2k** 1 year, 6 months ago

A

1. Each on-premises router is configured with a unique ASN = 2 Routers with 2 different ASNs. Let's assume that this router connects to the same Core Switch, it is like Triangle Architecture.

2. Each on-premises router is configured with the same routes and priorities. From inside on-premise, assuming they use BGP also, BGP will find the best path. So let's assume that.

How BGP finds the best path = <https://networklessons.com/bgp/bgp-attributes-and-path-selection>

Attributes

Weight

Local Preference

Origin

AS path length > As case "Each on-premises router is configured with a unique ASN". So BGP will find the shortest route as possible for this.

Origin code

MED

eBGP path over iBGP path

Shortest IGP path to BGP next hop

Oldest Path

Router ID

Neighbor IP address

<https://networklessons.com/bgp/how-to-configure-bgp-as-path-prepend>



upvoted 3 times

  **sagitarious2k** 1 year, 6 months ago

Well, scratch that. I just explained answer 'D' at above.

So 'D' is true.

upvoted 4 times

  **Jos** 1 year, 6 months ago

I think it should be D, why not? thanks

upvoted 1 times



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.

  **superpane** Highly Voted 1 year, 2 months ago

Correct is B and D.

After you order an interconnect, Google sends you and the NOC (technical contact) an email with your LOA-CFAs (one PDF file per interconnect). You must send these LOA-CFAs to your vendor so that they can install your cross connects. If you don't, your interconnects won't get connected. <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/retrieving-loas>

upvoted 13 times

  **Alex0303** 7 months, 4 weeks ago

For the Interconnect connection that contains the LOA-CFAs that you need, select the options button, and then select Download LOA-CFA. For B.

upvoted 1 times

  **Jerrard** Highly Voted 1 year, 3 months ago

Correct Answer is: B and D

upvoted 7 times

  **kumarp6** Most Recent 1 week, 1 day ago

Answer is : B and D

upvoted 1 times

  **desertlotus1211** 2 weeks ago

Answers are B&E: <https://docs.packetfabric.com/cloud/google/dedicated/create/>  
The NOC or technical contact [this will be your vendor] will be emailed the LOA-CFA

upvoted 1 times

  **Madhu73** 1 month, 3 weeks ago

LoA cannot be downloaded. When the LOA arrives, it is attached to an email. Looks like D, E are correct.

upvoted 1 times

  **Madhu73** 1 month, 3 weeks ago

Sorry about the LoA download above. Cloud doc shows that "If you can't find the LOA-CFAs in your email, retrieve them from the Google Cloud Console." Search for retrieving-loas in google cloud doc.

upvoted 1 times

  **PeppaPig** 4 months ago



E is wrong, LOA-CFAs will NOT be automatically emailed to vendors. You need to send them on your own

upvoted 1 times

  **[Removed]** 9 months ago

DE is just correct according to the reference, you just need to do two things ,first check the NOC account's email sent from google , then forward the LOA to your vendor <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/retrieving-loas>

upvoted 1 times

  **mwellger** 9 months, 2 weeks ago

For me the correct choice is D & E, you have to send the LOA-CFAs to your provider, the assumption here would be that you forward the email on to the provider. Answer B is the alternative if you can't find the email.

upvoted 4 times

  **Vidyasagar** 9 months, 3 weeks ago

Answers are B & D



upvoted 2 times

  **sc00by** 9 months, 2 weeks ago

B is not correct because by default, Google sends you the LOA-CFAs by email automatically, on the other hand, the question states that "need to give the Letter of Authorization/Connecting Facility Assignment (LOA-CFA) to your cross-connect provider", so in other words, you already have the LOA-CFAs.



upvoted 2 times

  **sc00by** 9 months, 2 weeks ago

D and E are best options.

upvoted 2 times

  **pentium2000** 9 months, 3 weeks ago


only B,D make sense

"After you order an Interconnect connection, Google emails you a confirmation and allocates ports for you. When the allocation is complete, Google generates LOA-CFAs for your connections and emails them to you.

All the automated emails are sent to the NOC contact and the email address of the Google Account used when ordering the Interconnect connection. You can also get your LOA-CFAs by using the Cloud Console.

You can use the Interconnect connection only after your connections have been provisioned and tested for light levels and IP connectivity."

upvoted 3 times

  **Ocedoc** 11 months, 2 weeks ago

As stated, "You ... need to give the LoA/CFA to you XC provider"

Answer:

B & E Download then contact XC provider.

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

"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."

Regarding D:

Checking the email for the account of the NOC contact doesn't accomplish anything. Instead, download the LOA-CFA from console and email to the cross-connect provider.

upvoted 2 times

  **groovygorilla** 1 year ago

B & D.

LOA-CFAs are not sent to vendor automatically by Google. Customer has to do it.

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

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.

upvoted 2 times

  **[Removed]** 1 year, 1 month ago

Ans - DE

upvoted 1 times

  **Aniyadu** 1 year, 3 months ago

B & D is the right answer.

upvoted 3 times

  **saaurabh1805** 1 year, 4 months ago

D and E are correct answer.

upvoted 2 times

  **saaurabh1805** 1 year, 4 months ago

I stand correct B and D is correct answer here.

"After you order an interconnect, Google emails you a confirmation and allocates ports for you. When the allocation is complete, Google generates LOA-CFAs for your cross connects and emails them to you.

All of the automated emails are sent to the NOC contact and the email of the Google account used when ordering the interconnect. You can also get your LOA-CFAs by using the console, see Retrieving LOA-CFAs."

upvoted 11 times

  **runtheworld** 1 year, 4 months ago

D,E should be the answer.

"After you order an interconnect, Google emails you a confirmation and allocates ports for you. When the allocation is complete, Google generates LOA-CFAs for your cross connects and emails them to you." <https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/ordering-dedicated-interconnect>

upvoted 2 times

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.

🗲️ 👤 **architect** Highly Voted 👍 1 year, 6 months ago

Definitely B.

It says you "believe" you have a bad actor, and want to confirm this "while minimizing disruption to your legitimate users."

[A] would block the traffic suspected IP, causing disruption to a legitimate user if you were wrong about the actor

[B] Correct - You can log the requests by Client IP, and Preview Mode will not cause disruption to anyone, while you investigate.

[C] Global Load balancers are Proxies, as Jordi says. This could work for Network load balancers, which are not proxies, but they are regional and not global.

[D] As above, even if you could block from an NLB, it would cause disruption to someone.

upvoted 17 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : B

upvoted 1 times

🗲️ 👤 **Madhu73** 1 month, 2 weeks ago

<https://jayendrapatil.com/tag/security-policies/>. This guy says B too.

upvoted 1 times

🗲️ 👤 **seddy** 8 months ago

B for sure. It is possible to deny traffic at VM level with firewall rules (firewall rules won't apply to a LB; LB will always allow a request unless there is a Cloud Armor policy). But firewall policies do not have a preview mode, only Cloud Armor does!

upvoted 3 times

🗲️ 👤 **[Removed]** 9 months ago

I voted for B

[https://cloud.google.com/armor/docs/security-policy-overview#preview\\_mode](https://cloud.google.com/armor/docs/security-policy-overview#preview_mode)

upvoted 2 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

B is the one

upvoted 1 times

🗲️ 👤 **voyager** 10 months, 2 weeks ago

It is "D". The malicious IP Address is know and with D the FW rule blocks only a sigle IP

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - B

upvoted 1 times

🗲️ 👤 **saurabh1805** 1 year, 4 months ago

B is correct answer.

upvoted 1 times

🗲️ 👤 **HateMicrosoft** 1 year, 4 months ago

The correct anwser is B.

Preview mode

[https://cloud.google.com/armor/docs/security-policy-concepts#preview\\_mode](https://cloud.google.com/armor/docs/security-policy-concepts#preview_mode)

upvoted 2 times

🗲️ 👤 **jordi\_194** 1 year, 7 months ago

For sure it's B. Firewall rules do not see client IPs in proxy LBs.

[https://cloud.google.com/armor/docs/security-policy-concepts#preview\\_mode](https://cloud.google.com/armor/docs/security-policy-concepts#preview_mode)

upvoted 4 times

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.

🗲️ 👤 **Jerrard** Highly Voted 👍 1 year, 3 months ago

Correct Answer: B  
upvoted 6 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : B  
upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks, 2 days ago

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

'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.'

upvoted 1 times

🗲️ 👤 **seddy** 8 months ago

B for sure. It cannot be a managed instance group bc we cannot scale unidentical VMs. We can either use an unmanaged instance group or a target pool (for only NW LBer)  
upvoted 4 times

🗲️ 👤 **EJJ** 8 months, 3 weeks ago

This question doesn't make sense. It states that the request to the backend server will have to go through a network load balancer. Backend server + network load balancer means this is internal TCP/UDP load balancer. Choices A and B is wrong since there is no Target Pool in Internal TCP/UDP load balancer, it only have Backend Service. Choice C is not correct also since it requires a GCP-native service. And choice D is all about routing and network connectivity, nothing to do with backend server and load balancer.

upvoted 1 times

🗲️ 👤 **pentium2000** 9 months, 3 weeks ago

I will go B, at least it makes sense.  
upvoted 2 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

B is Correct  
upvoted 2 times

🗲️ 👤 **eeghai7thioyaiR4** 10 months, 2 weeks ago

None of these answers looks good to me

We have many backend servers, with different configuration, so they are not interchangeable : some of them are for a specific purpose, while other are for another purpose

So:

A: create a managed instance group: while we could "tune" the newly created instances using boot script, this is useless, see B

B. Create a target pool, add all backend instances, deploy the pool behind a proxy. All requests will be randomly spread across all backend, which means that backends specificities will be ignored. Not a solution.

C. Sounds awful, yet it will work : that blackbox will understand your config differencies and will have the required knowledge to route the requests to the right backend

D. Same thing as A or B: random dispatch won't work

So .. out of disgust, I'll go with C

upvoted 2 times

  **[Removed]** 1 year, 1 month ago

Ans - B

upvoted 1 times

  **saurabh1805** 1 year, 4 months ago

B Seems to be correct answer, Since all servers have slight different configuration that means manage instance group cant be used here.

upvoted 1 times

Question #19

Topic 1

You decide to set up Cloud NAT. After completing the configuration, you find that one of your instances is not using the Cloud NAT for outbound NAT.

What is the most likely cause of this problem?

- A. The instance has been configured with multiple interfaces.
- B. An external IP address has been configured on the instance.
- C. You have created static routes that use RFC1918 ranges.
- D. The instance is accessible by a load balancer external IP address.

  **saurabh1805** Highly Voted  1 year, 4 months ago

B is correct answer.

upvoted 5 times

  **kumarp6** Most Recent  1 week, 1 day ago



Answer is : B

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Ans - B

upvoted 2 times

  **Jerrard** 1 year, 3 months ago

Correct Answer: B

upvoted 2 times

  **iobluedot** 1 year, 4 months ago

This is why <https://cloud.google.com/nat/docs/overview#specifications>

"The existence of an external IP address on an interface always takes precedence and always performs one-to-one NAT, without using Cloud NAT."

upvoted 2 times

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

🗨️ 👤 **kumarp6** 1 week, 1 day ago

Answer is : D  
upvoted 1 times

🗨️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is correct  
upvoted 4 times

🗨️ 👤 **BobBui** 10 months, 1 week ago

The right answer is D, <https://cloud.google.com/network-connectivity/docs/router/concepts/overview#route-metric-examples>  
upvoted 1 times

🗨️ 👤 **densnoigaskogen** 1 year ago

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.  
Ref: <https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/13759-37.html>  
upvoted 1 times

🗨️ 👤 **densnoigaskogen** 1 year ago

I was struggling with choosing between A and D. Because BGP selects shortest AS path first when sending traffic. In our On-prem router, we can actually prepend AS path for the standby BGP session. However, after learning from GCP's documentations(as referenced below) that GCP uses MED to set base priority. I decided to choose D.  
Additional ref: <https://cloud.google.com/network-connectivity/docs/router/concepts/overview#route-metrics>  
[https://cloud.google.com/network-connectivity/docs/router/concepts/overview#suggested\\_base\\_priority\\_values](https://cloud.google.com/network-connectivity/docs/router/concepts/overview#suggested_base_priority_values)  
upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D  
upvoted 1 times

🗨️ 👤 **Windows98** 1 year, 2 months ago

D - Med.

Configuring devices for active/passive forwarding

Make sure that higher MED values are applied on the Cloud Router side, and on the on-premises device side, to avoid asymmetric routing  
upvoted 1 times

🗨️ 👤 **saurabh1805** 1 year, 4 months ago

D is correct answer here, Refer below link to refer

<https://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/112965-bgpmed-attr-00.html>  
upvoted 3 times

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.

🗲️ 👤 **HateMicrosoft** Highly Voted 👍 1 year, 4 months ago

The correct answer is C

Option 1: Scale the on-premises VPN gateway

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#option-1>

upvoted 7 times

🗲️ 👤 **seddy** Highly Voted 👍 8 months ago

Answer is 100% C!

There is practically no difference between C and D in terms of increasing the throughput. However, D does not work due to one info given in the statement. 'create a secondary VPN gateway in a DIFFERENT region'. The secondary VPN gateway should be in the same region as the first VPN gateway in order for this method to work.

upvoted 5 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **JohnnyBG** 5 months, 3 weeks ago

I wonder why nobody thinks it's B. From Cloud Guru's video, they clearly state that we can create multiple tunnels in order to increase the bandwidth.

upvoted 4 times

🗲️ 👤 **desertlotus1211** 2 weeks ago

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#option-1>

This shows you need TWO Cloud VPN gateways... Answer B is only using ONE Cloud VPN GW...

upvoted 1 times

🗲️ 👤 **brtest** 1 month ago

You should trust at GCP Documentation: <https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#option-1>, rather than Cloud Guru's Video!

upvoted 2 times

🗲️ 👤 **EJJ** 8 months, 3 weeks ago

Ans C and D are correct

Option 1: Scale the on-premises VPN gateway.

Option 2: Scale the Cloud VPN gateway. If your on-premises VPN gateway's throughput capabilities are higher, and you want to scale higher throughput from the Cloud VPN gateway, you can set up a second Cloud VPN gateway.

Option 3: Scale both the on-premises VPN gateway and the Cloud VPN gateway.

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

upvoted 1 times

🗲️ 👤 **EJJ** 8 months, 3 weeks ago

I believe the final answer is D since the question mentioned specifically that you wanted to "increase the available bandwidth using CLOUD VPN", not using "on-premise VPN gateway"

upvoted 1 times

🗲️ 👤 **matmuh** 1 month ago

D is impossible. You should not use two different regions for increasing bandwidth.

upvoted 1 times

🗲️ 👤 **Even** 8 months, 2 weeks ago

Answer D is totally wrong. Second Cloud VPN Gateway should be created in the same region, not different region.

<https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#option-2>

Add a second Cloud VPN gateway in the same region as the existing VPN gateway. The second Cloud VPN gateway can have a tunnel that points to the same IP address of the on-premises VPN gateway as the tunnel on the first gateway





upvoted 2 times

  **Even** 8 months, 2 weeks ago

Final answer is C

upvoted 2 times

  **Vidyasagar** 9 months, 3 weeks ago

C is right

upvoted 1 times

  **densnoigaskogen** 1 year ago

The answer is C.

Based on the answer options, this question is testing us 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.

upvoted 2 times

  **densnoigaskogen** 1 year ago

2. Scale the Cloud VPN gateway. Adding a second Cloud VPN gateway in the SAME region as the existing VPN gateway, because Cloud VPN gateways are regional service. The second Cloud VPN gateway can have a tunnel that points to the same IP address of the on-premise VPN gateway as the tunnel on the first gateway. Once configured, traffic to the on-premises VPN gateway is automatically load balanced between the two Cloud VPN gateways and tunnels. Thus, D is wrong.

3. Combine both options 1 and 2 above to provide so-called 'bow-tie' setup.

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

upvoted 3 times

  **groovyorilla** 1 year ago

C should be the right answer since the following doc rules out the possibility of B:

<https://cloud.google.com/network-connectivity/docs/vpn/how-to/adding-a-tunnel#adding-a-tunnel-classic>

"Each Cloud VPN tunnel associated with a Classic VPN gateway must connect to a unique peer VPN gateway, as identified by the peer gateway's IP address. If you need to create a second tunnel to the same peer gateway, you must create that tunnel from a different Cloud VPN gateway."

upvoted 1 times

  **Gharet** 1 year ago

If you need to create a second tunnel to the same peer gateway, you must create that tunnel from a different Cloud VPN gateway. Seems to me it may be D?

upvoted 1 times

  **Gharet** 1 year ago


Sorry i believe it's C, as you are adding the second gateway in C

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 1 times

  **jonclem** 1 year, 2 months ago


Personally, I'd go with the original answer, B. Option C would appear to be a "fail-over/HA" type of configuration and not one that "supports more traffic" as the question asks.

upvoted 1 times

  **nikiwi** 1 year, 1 month ago



yup I agree, they just asked for more traffic capacity and B is the simplest solution.

upvoted 1 times

  **beebee** 1 year, 5 months ago

Should be C

upvoted 1 times

  **dxloader** 1 year, 6 months ago

C is correct

upvoted 1 times



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.

🗲️ 👤 **saurabh1805** Highly Voted 👍 1 year, 4 months ago

C is correct answer here.

upvoted 5 times

🗲️ 👤 **saurabh1805** 1 year, 4 months ago

refer below link for more details

<https://cloud.google.com/dns/docs/registrars#del-ds>

upvoted 2 times

🗲️ 👤 **HateMicrosoft** 1 year, 4 months ago

Deactivating DNSSEC at your Domain Registrar

<https://cloud.google.com/dns/docs/registrars#del-ds>

upvoted 6 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 4 times

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.

🗲️ 👤 **EJJ** Highly Voted 👍 8 months, 3 weeks ago

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.

upvoted 10 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks, 2 days ago

Answer is C: communication is initiated from outside.... Which means it is INGRESSING... VPC flow logs are enabled, too.

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

'Ingress packets are sampled after ingress firewall rules. If an ingress firewall rule denies inbound packets, those packets are not sampled by VPC Flow Logs.'

upvoted 1 times

🗲️ 👤 **JoeShmoe** 7 months, 2 weeks ago

Its C, the traffic is initiated from outside the subnet. It is able to egress so the ingress rule must be failing or is incorrect

upvoted 2 times

🗲️ 👤 **KDMIndia** 7 months, 3 weeks ago

I would go for Answer : D. As "instance that cannot communicate with a resource outside of its subnet". Which talked about egress traffic.

upvoted 2 times

🗲️ 👤 **paweu** 7 months, 3 weeks ago

The easier version of EJJ -

your traffic that is stopped by basic deny all rule (default one) in firewall is never logged anywhere.

Traffic needs to hit some rule to be logged, best way around is to create deny all rule just some spaces higher than default one

upvoted 1 times

🗲️ 👤 **WakandaF** 8 months, 3 weeks ago

Why the The traffic is matching the expected ingress rule?

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

Answer is C

upvoted 1 times

🗲️ 👤 **AnasAloan84** 9 months, 3 weeks ago

Ans - A

as ç The external resource initiates communication., then the response traffic "egress" will not be logged. so as traffic match ingress rules, the egress traffic will not be logged.

upvoted 2 times

🗲️ 👤 **mamh** 10 months ago

I'm going to C.

Will have ingress log if matched one of the ingress rules (except the deny all implied rule )

upvoted 1 times

🗨️ 👤 **Ocedoc** 11 months, 2 weeks ago

I'm going to suggest D.

The resource with which the VM cannot communicate is external to the subnet. All firewall rules in the VPC subnet are set to log, HOWEVER logging cannot be enabled for the implied 'allow all egress' or the implied 'deny all ingress'. So perhaps the traffic is not matching the expected egress rule and is instead being allowed by the implied 'allow all egress' rule, hence not being logged. Traffic being allowed out of the subnet is a reasonable cause for a missing firewall log line.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 1 times

🗨️ 👤 **ravirajani** 1 year, 4 months ago

Since External resource initiates traffic, its incoming. And its blocked, so Incoming is not matching the existing firewall rules. Hence, C

upvoted 4 times

🗨️ 👤 **buldas** 8 months, 4 weeks ago

If it would be blocked i t would be logged, so the only one answer remaining is A

upvoted 1 times

🗨️ 👤 **Ocedoc** 11 months, 2 weeks ago

Why is it not logged?

upvoted 1 times

🗨️ 👤 **cyma** 6 months, 3 weeks ago

it is blocked by default deny rule. (all ingress is deny by default). default rule is not logged.

upvoted 2 times

Question #24

Topic 1

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

What is the most likely cause of the problem?

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

🗨️ 👤 **kumarp6** 1 week, 1 day ago

Answer is : D

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D

upvoted 3 times

🗨️ 👤 **saaurabh1805** 1 year, 4 months ago

D is correct answer here, refer below link for more details.

<https://cloud.google.com/cdn/docs/troubleshooting-steps#compression-not-working>

upvoted 3 times

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.

🗲️ 👤 **kumarp6** 1 week, 1 day ago

Answer is : B  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

B is the one  
upvoted 3 times

🗲️ 👤 **eeghai7thioyaiR4** 10 months, 2 weeks ago

An HTTP load balancer may help a bit

While the speed of light will be unchanged (US <-> asia is a long trip), users will connect to the http load balancer  
An tcp connection uses a 3 way handshake, so additionnal roundtrip are required  
But http load balancers uses keepalived, so connections to the origin are kept across requests

So, instead of cust <-> US (2 long RTT), you get cust <-> asia (2 small RTT) + asia <-> US (1 long RTT)  
upvoted 1 times

🗲️ 👤 **densnoigaskogen** 1 year ago

Answer is B.  
Network LB is regional service. This scenario requires global scale type of LB, thus HTTP LB is the correct choice.  
upvoted 1 times

🗲️ 👤 **Gharet** 1 year ago

B is correct  
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - B  
upvoted 1 times

🗲️ 👤 **saurabh1805** 1 year, 4 months ago

B is correct answer here.  
upvoted 3 times

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.

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

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>

upvoted 15 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : A and E

upvoted 1 times

🗲️ 👤 **SonamDhingra** 2 weeks, 4 days ago

Selected Answer: AE

A & E please

upvoted 1 times

🗲️ 👤 **Arad** 1 month, 3 weeks ago

A & E are correct.

upvoted 1 times

🗲️ 👤 **[Removed]** 8 months, 4 weeks ago

Because Private Google Access is enabled on a per-subnet basis, you must use a VPC network. So choose A over B

upvoted 3 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

A and E

upvoted 1 times

🗲️ 👤 **groovygorilla** 1 year ago

Shoube be AE because Private Google Access is enabled at the subnet level.

upvoted 1 times

🗲️ 👤 **gless** 1 year ago

I would go with C and E since here --> Private Google Access <https://cloud.google.com/vpc/docs/configure-private-google-access#specifications> is written:

"The primary internal IP address of a VM's network interface in an enabled subnet Except if that interface has an external address assigned".

upvoted 1 times

🗲️ 👤 **nikiwi** 1 year, 1 month ago

A&E is correct by method of elimination,

but can somebody explain how E would help with "You want to ensure that none of the application instances have external IP addresses." ?

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - AE

upvoted 1 times

🗲️ 👤 **alexv** 11 months, 1 week ago

private google access turning on at the vpc level

upvoted 1 times

🗲️ 👤 **alexv** 11 months, 1 week ago

sorry i am not right

upvoted 1 times

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.

  **kumarp6** 1 week, 1 day ago

Answer is : D



upvoted 1 times

  **densnoigaskogen** 7 months, 4 weeks ago

D is the answer.

The question wants us to follow Google's recommended practice, keeping it simply is one of the key best practices. Thus, creating ONLY 1 Shared VPC in the host project makes it easier to centralize and manage network resources (such as subnets, routes, and security rules) for the attached service VPCs.

upvoted 4 times

  **Vidyasagar** 9 months, 3 weeks ago

D is correct

upvoted 2 times

  **Gharet** 1 year ago


D is the correct answer

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Ans - D

upvoted 1 times

  **ESP\_SAP** 1 year, 2 months ago

Correct Answer (D):

Building on the initial reference architecture, Shared VPC host projects and multiple service projects let administrators delegate administrative responsibilities—such as creating and managing instances—to Service Project Admins while maintaining centralized control over network resources like subnets, routes, and firewalls.

<https://cloud.google.com/solutions/best-practices-vpc-design#single-host-project-multiple-service-projects-single-shared-vpc>

upvoted 4 times

  **maxrh** 5 months ago




I dont understand how would the 2 networks communicate over a dedicated network then?




you can separate them with sharing a specific subnet for each but how would they communicate then ?




upvoted 1 times



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.



  **Barry123456** Highly Voted  1 year, 6 months ago  
Who posts these answers? It's C!  
upvoted 21 times



  **mozammil89** Highly Voted  1 year, 10 months ago  
Correct answer is C  
upvoted 9 times



  **kumarp6** Most Recent  1 week, 1 day ago  
Answer is : C  
upvoted 1 times



  **yas\_cloud** 1 week, 2 days ago  
Selected Answer: C  
Answer should be C.  
upvoted 1 times



  **SonamDhingra** 2 weeks, 4 days ago  
Selected Answer: C  
Who posts these answers? It's C!  
upvoted 1 times



  **Arad** 1 month, 3 weeks ago  
Definitely C is correct.  
upvoted 1 times

  **Arvinder** 7 months, 3 weeks ago  
Indeed, it' C.  
upvoted 4 times

  **[Removed]** 8 months, 4 weeks ago  
I agree with C. least priviledge.  
upvoted 1 times

  **Vidyasagar** 9 months, 3 weeks ago  
Correct Answer is C  
upvoted 1 times

  **pentium2000** 9 months, 3 weeks ago  
C indeed.  
upvoted 1 times

  **[Removed]** 1 year, 1 month ago  
Ans - C  
upvoted 3 times



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.

🗲️ 👤 **[Removed]** Highly Voted 👍 1 year, 1 month ago  
Ans - D  
upvoted 7 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago  
Answer is : D  
upvoted 1 times

🗲️ 👤 **ThisisJohn** 2 months, 2 weeks ago  
My vote goes to D as well.

"After you convert an auto mode network to custom mode, you must review all API calls and gcloud commands that implicitly reference any subnet that was automatically created while the network was in auto mode. API calls and commands will need to be modified so that they reference the subnet explicitly." <https://cloud.google.com/vpc/docs/using-vpc#switch-network-mode>  
upvoted 1 times

🗲️ 👤 **ESP\_SAP** 1 year, 2 months ago  
Correct Answer is (D):

All yaml files used by Deployment Manager as template used to resources provisioning, must be updated manually.  
upvoted 2 times

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.

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago  
Correct Answer are (D) & (E)

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>  
upvoted 10 times

🗲️ 👤 **dzhu** 3 months, 3 weeks ago  
E is not scripting and automation. So E is obviously wrong. The answer should be B and D  
upvoted 1 times

🗲️ 👤 **[Removed]** Highly Voted 👍 1 year, 1 month ago  
Ans - DE  
upvoted 6 times

🗲️ 👤 **ThisisJohn** Most Recent 🕒 2 months, 2 weeks ago  
I'd vote A and B as @EranSolstice says, because of the following except from here <https://cloud.google.com/iam/docs/granting-changing-revoking-access#multiple-roles>

To make large-scale access changes that involve granting and revoking MULTIPLE roles, use the read-modify-write pattern to update the resource's IAM policy:

Reading the current policy by calling getIamPolicy().  
Editing the returned policy, either by using a text editor or programmatically, to add or remove any principals or role bindings.  
Writing the updated policy by calling setIamPolicy().  
upvoted 1 times

🗲️ 👤 **ThisisJohn** 2 months, 2 weeks ago  
I'd vote A and B as @EranSolstice says, because of the following except from here <https://cloud.google.com/iam/docs/granting-changing-revoking-access#multiple-roles>

To make large-scale access changes that involve granting and revoking MULTIPLE roles, use the read-modify-write pattern to update the resource's IAM policy:

Reading the current policy by calling getIamPolicy().  
Editing the returned policy, either by using a text editor or programmatically, to add or remove any principals or role bindings.  
Writing the updated policy by calling setIamPolicy().  
upvoted 1 times

🗲️ 👤 **EranSolstice** 2 months, 3 weeks ago  
A) GetIamPolicy() would not do anything by itself but see (B)  
B) would require use of GetIamPolicy() as otherwise SetIamPolicy() override existing binding  
C) obviously wrong, question is not about pubsub  
D) the documentation indicate that project\_id need to be used not project\_name, would therefore return an error  
E) would work, despite being very vague, but is not automation.

Now, the question ask for "which 2 \_methods\_ can be used to achieve that".

Both GetIamPolicy() and SetIamPolicy() are programatic \_methods\_ that if used together could achieve that.

Therefore one could roll with A&B in the spirits of that very tricky question.  
upvoted 3 times

🗲️ 👤 **PeppaPig** 4 months, 1 week ago  
B&D are correct.  
upvoted 2 times



  **JohnnyBG** 6 months ago

Tricky question, I would say B and D since automation is the preferred choice. But for B, see below .. probably better than manually as in E but it implies that you have all other IAM Setting and apply them all together ..

CAUTION: This method will replace the existing policy, and cannot be used to append additional IAM settings.

<https://cloud.google.com/resource-manager/reference/rest/v1/projects/setIamPolicy>

upvoted 2 times

  **Fliu** 6 months, 3 weeks ago

D is incorrect:

members[]

string

user:{emailid}: An email address that represents a specific Google account. For example, alice@example.com .


<https://cloud.google.com/iam/docs/reference/rest/v1/Policy#Binding>

upvoted 1 times

  **ExamTopicsFan** 3 months, 2 weeks ago



gcloud projects add-iam-policy-binding example-project-id-1 --member='user:test-user@gmail.com' --role='roles/editor'

upvoted 1 times

  **Fliu** 6 months, 3 weeks ago

AB will be the answer

upvoted 1 times

  **EJJ** 8 months, 3 weeks ago

Ans is BD.. take note that the preferred way is thru automation using scripting

upvoted 4 times

  **Vidyasagar** 9 months, 3 weeks ago

D and E

upvoted 4 times

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]`.

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago  
Correct Answer is (A)

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 .

upvoted 7 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago  
Answer is : A  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago  
A is correct  
upvoted 2 times

🗲️ 👤 **Gharet** 1 year ago  
Correct Answer is (A) its the only logical solution as its truly the limiting factor here.  
upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - A  
upvoted 2 times

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.

  **ESP\_SAP** Highly Voted  1 year, 2 months ago

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  
upvoted 16 times

  **desertlotus1211** 2 weeks ago

You're mistaken VPC and VPC Networks.

'A project that participates in Shared VPC is either a host project or a service project:

A host project contains one or more Shared VPC networks'...

Each VPC Network has subnets.... The appliance NIC can attach to each subnet...

The answers are misleading as it says 'VPC' do they mean VPC Network OR literally another VPC - which in any event is another set of network subnets...

There is no need for TWO VPC Networks... therefore Answer is C.

Thoughts?

upvoted 1 times

  **desertlotus1211** 2 weeks ago

Unless they refer to VPC as a subnet - which is dumb ;)

upvoted 1 times

  **walkwolf3** 3 weeks, 6 days ago

Shared networks should be created in the host project, while shared instances should be created in the service project and connected to shared networks to communicated with other parties. Answer B is correct.

upvoted 1 times

  **seddy** 8 months ago

Yeah, but I believe the Centralized network Administration refers to 'Shared VPC' in general, not to creating the workload in the Host project. By creating a shared VPC, we are centralizing the networking aspect in the first place. Then, it's a best practice to separate the workload by creating the instance in the service project.

So, I believe the answer should be B!  
upvoted 5 times

  **kumarp6** Most Recent ↻ 1 week, 1 day ago

Answer is : A  
upvoted 1 times

  **matmuh** 1 month ago

Answer is B.



Why not option A? Because installing all projects on the shared vpc host project does not comply with google's best practices.  
upvoted 1 times

  **densnoigaskogen** 7 months, 4 weeks ago



C should be the answer.  
It's about using 3rd party appliances in a Shared VPC network scenario.  
"Centralized Anetwork Administration Team" indicates that we need to have contralised control for network resources( such as, subnets, routes, firewall rules), a single VPC in shared VPC Host project is the best choice of architecure.  
In a shared VPC network, we can create a VM with mulitple network interfaces attaching to different subnets, which represent different networks.  
Reference: <https://cloud.google.com/vpc/docs/multiple-interfaces-concepts#third-party>  
upvoted 2 times

  **densnoigaskogen** 7 months, 4 weeks ago

Reviewed the question again, my answer is wrong.  
A should be the answer. The reasons to create 2 VPCs in the shared VPC Host project can be:  
- meet the requirements of primary and backup redundancy for interconnect towards the Data centers in Oregon and New york. Each VPC should represent a On-prem Data Center.  
- each VM NIC needs to be attached to a VPC, as we can not attach multiple network interfaces of a VM to the same VPC network.  
B is not correct, because the L7 virutal application needs to be deployed in Host project to bridge between those 2 VPCs, so that it can inspects both traffic coming from interconnects (us-west1 and us-east4) and internet-based connections (Europe and APAC)  
Additonal ref: <https://cloud.google.com/architecture/best-practices-vpc-design#single-host-project-multiple-service-projects-single-shared-vpc>  
upvoted 2 times

  **WakandaF** 8 months, 3 weeks ago



So! will be A or B?  
upvoted 1 times

  **Vidyasagar** 9 months, 3 weeks ago

B is correct  
upvoted 2 times

  **[Removed]** 1 year, 1 month ago

Ans - B  
upvoted 1 times

  **majun** 1 year, 2 months ago

The correct answer should be B.  
In the shared VPC scenario, Host Project is the deployment of the VPC network, and Service Project is the deployment of the instance.

<https://cloud.google.com/vpc/docs/shared-vpc>  
upvoted 2 times

  **ThisisJohn** 1 month, 3 weeks ago

Definitely, as Hybrid\_Cloud\_boy says, you can deploy instances into a host project, as per the example below:

Stateful L7 firewall between VPC networks <https://cloud.google.com/architecture/best-practices-vpc-design#l7>  
upvoted 1 times

  **Hybrid\_Cloud\_boy** 1 year, 1 month ago

You can absolutely deploy instances into a host project - This is incorrect. A is the right answer.  
upvoted 2 times

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.

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

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>

I think the correct answer is A since:

GKE is expected to grow 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)

upvoted 18 times

🗲️ 👤 **walkwolf3** 3 weeks, 5 days ago

Agreed A.

When you create a VPC-native cluster, you specify a subnet in a VPC network. The cluster uses three unique subnet IP address ranges:

It uses the subnet's primary IP address range for all node IP addresses.

It uses one secondary IP address range for all Pod IP addresses.

It uses another secondary IP address range for all Service (cluster IP) addresses.

[https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster\\_sizing](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster_sizing)

upvoted 1 times

🗲️ 👤 **Hybrid\_Cloud\_boy** Highly Voted 👍 1 year, 1 month ago

Isn't max pods per node 110 in VPC native? I don't understand how the scenario painted by the question is even possible when taking that into consideration.

upvoted 6 times

🗲️ 👤 **ThisisJohn** 1 month, 3 weeks ago

Agree with you.

"This table assumes the maximum number of Pods per node is 110 (the default and largest possible Pod density)."

Ref. [https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster\\_sizing\\_secondary\\_range\\_pods](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster_sizing_secondary_range_pods)

upvoted 2 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : A

upvoted 1 times

🗲️ 👤 **ThisisJohn** 2 months, 2 weeks ago

I don't think it can be A because Google recommends a subnet not smaller than /21 for pods. My vote goes for B

If you specify a Pod address range smaller than a /21 range, you risk running out of Pod IP addresses as your cluster grows

[https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster\\_sizing](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster_sizing)

upvoted 1 times

🗲️ 👤 **ThisisJohn** 1 month, 3 weeks ago

Let me correct myself.

A /24 subnet cannot host 1500 services, so answer should be A

upvoted 1 times

🗲️ 👤 **[Removed]** 8 months, 4 weeks ago

I agree with A



upvoted 1 times

  **Vidyasagar** 9 months, 3 weeks ago

A is correct

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Ans - A

upvoted 3 times

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

  **densnoigaskogen** Highly Voted 7 months, 4 weeks ago

D should 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>

upvoted 11 times

  **BobBui** Highly Voted 10 months ago

I go with D, <https://cloud.google.com/load-balancing/docs/choosing-load-balancer>

SSL offload yes >> SSL proxy



SSL offload no >> TCP proxy

upvoted 7 times

  **kumarp6** Most Recent 1 week, 1 day ago

Answer is : D

upvoted 1 times

  **desertlotus1211** 2 weeks, 2 days ago

Answer is D.

Answer A is wrong BECAUSE their is on SSL traffic coming in [SMTP & IMAP]. Nor does the question say SSL is being sent...

They have no SSL Certs so why are you using SSL proxy LB?

upvoted 1 times

  **SonamDhingra** 2 weeks, 4 days ago

A

Certificate management. Your customer-facing SSL certificates can be either certificates that you obtain and manage (self-managed certificates), or certificates that Google obtains and manages for you (Google-managed certificates). Google-managed SSL certificates each support up to 100 domains. Multiple domains are supported for Google-managed certificates. You only need to provision certificates on the load balancer. On your VMs, you can simplify management by using self-signed certificates.

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

upvoted 1 times

  **PeppaPig** 4 months, 1 week ago

A is correct. Without access to Cert how would you be able to upload cert to your backend servers? Thus D is Wrong.

It has nothing to do with SSL offloading, and encryption Does NOT necessarily mean SSL encryption

For SSL proxy LB, Google automatically encrypts traffic between Google Front Ends (GFEs) and backends that reside within Google Cloud VPC networks. This is a network-level encryption. In addition to network-level encryption, you can use a secure protocol such as SSL

[https://cloud.google.com/load-balancing/docs/ssl-certificates/encryption-to-the-backends#encryption\\_between\\_gfes\\_and\\_backends](https://cloud.google.com/load-balancing/docs/ssl-certificates/encryption-to-the-backends#encryption_between_gfes_and_backends)

upvoted 3 times

  **ThisisJohn** 1 month, 3 weeks ago



I'm not sure but I believe users connecting may receive a security warning, since they'll see a Google-managed certificate instead of the expected service certificate

upvoted 1 times

  **JohnnyBG** 6 months ago

Answer is A, using managed cert you do not need to have your own. TCP/SSL proxy act as a proxy (duh), therefore it can't be TCP Proxy. HTTPS is for HTTP protocol only and network LB is regional only.

upvoted 2 times

  **jdjorge** 8 months, 3 weeks ago

is option A. TCP proxy for unencrypted well known ports like smtp but ssl when using those same ports with encryption

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

upvoted 2 times

  **WakandaF** 8 months, 3 weeks ago

I'll go D.  
A. SSL proxy load balancer - wrong - it needs to go end-to-end encryption, which means traffic is not off-loaded on LB.  
B. Network load balancer - wrong - it doesn't support global load balancing.  
C. HTTPS load balancer - wrong. it only works on HTTP(s) protocols.  
D. TCP proxy load balancer - I will go this on


D is the correct one?

upvoted 2 times

  **[Removed]** 8 months, 4 weeks ago



I support D, as you do not have access to the certificate, so can not use SSL offload, then can not use A.

upvoted 2 times

  **mwellger** 9 months, 1 week ago

I think the correct answer would be A (SSL) and I believe that to be the case because it supports TCP 25/110 & to support not having access to the SSL Certs, I think in this situation they are using Google managed SSL certs.

upvoted 2 times

  **sc00by** 9 months, 2 weeks ago

Option B is correct answer. The only option to handle end-to-end SSL traffic without terminating traffic at the proxy level.

Accroding to: <https://cloud.google.com/load-balancing/docs/network>

#####

It is acceptable to have SSL traffic decrypted by your backends instead of by the load balancer. The network load balancer cannot perform this task. When the backends decrypt SSL traffic, there is a greater CPU burden on the VMs.

#####

upvoted 2 times

  **pentium2000** 9 months, 3 weeks ago

I'll go D.  
A. SSL proxy load balancer - wrong - it needs to go end-to-end encryption, which means traffic is not off-loaded on LB.  
B. Network load balancer - wrong - it doesn't support global load balancing.  
C. HTTPS load balancer - wrong. it only works on HTTP(s) protocols.  
D. TCP proxy load balancer - I will go this one.

upvoted 2 times

  **Vidyasagar** 9 months, 3 weeks ago



A is the correct answer

upvoted 2 times

  **porsak** 11 months ago

It is D in my opinion.  
You can't use SSL with SSL offload because you don't have access to any certificate.  
And TCP LB support end-to-end encryption just with no SSL offload.  
Network is regional.  
HTTPS use 80 and 443 ports only.

upvoted 4 times

  **chetz12** 11 months, 2 weeks ago

Network LB: Not global  
HTTPS : Only for http(s) traffic  
TCP : supports the messaging protocols but not e2e encryption  
SSL: Supports the protocols and encrypt  
So correct is "A"

upvoted 2 times

  **groovyygorilla** 1 year ago

I would choose D.

upvoted 2 times

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

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

Correct Answer are (A) & (C):

The solution is incorrect. GCP recommends creating VPC peering for establishing communication between two organizations in GCP.  
upvoted 18 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : A and C  
upvoted 1 times

🗲️ 👤 **JesusMariaJose** 1 month, 3 weeks ago

Selected Answer: CD

Vote CD. Note that on VPC Peering it is not possible to select which subnet has access to what between subnets. Thus there is a security risk of sharing information between orgs / projects.  
upvoted 2 times

🗲️ 👤 **desertlotus1211** 2 weeks, 2 days ago

You clearly don't know what Dedicated Interconnects are...  
upvoted 1 times

🗲️ 👤 **lehnnon1925** 1 month, 2 weeks ago

anyone have taken the exam recently and can confirm that all the questions here are still valid?  
upvoted 3 times

🗲️ 👤 **akg001** 1 month, 2 weeks ago

I am also trying to figure out this.  
upvoted 3 times

🗲️ 👤 **Arad** 1 month, 3 weeks ago

A & C are correct.  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

A & C are correct  
upvoted 2 times

🗲️ 👤 **pentium2000** 9 months, 3 weeks ago

AC 200%  
upvoted 1 times

🗲️ 👤 **cesar7816** 1 year, 1 month ago

A and C, Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization.  
upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - AC  
upvoted 4 times

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.

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

Correct Answer is (B):

You might want to remove an object from the cache prior to its normal expiration time. You can force an object or set of objects to be ignored by the cache by requesting a cache invalidation.

Path patterns

Each invalidation request specifies a path pattern that identifies the object or set of objects that should be invalidated. The path pattern can be either a specific path, such as /cat.jpg, or an entire directory structure, such as /pictures/\*. The following rules apply to path patterns:

The path pattern must start with /.

It cannot include ? or #.

It must not include an \* except as the final character following a /.

If it ends with /\*, the preceding string is a prefix, and all objects whose paths begin with that prefix are invalidated.

upvoted 16 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : B

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks, 2 days ago

Answer is B: [https://cloud.google.com/cdn/docs/invalidating-cached-content#gcloud\\_1](https://cloud.google.com/cdn/docs/invalidating-cached-content#gcloud_1)

Invalidate the whole directory

gcloud compute url-maps invalidate-cdn-cache LOAD\_BALANCER\_NAME \

--path "/images/\*"

upvoted 1 times

🗲️ 👤 **Raghucs** 2 months, 2 weeks ago

Ans - B

upvoted 1 times

🗲️ 👤 **groovygorilla** 1 year ago

It should be "B", the invalidation method is taught in the coursera course.

upvoted 2 times

🗲️ 👤 **cesar7816** 1 year, 1 month ago

Ans is B, <https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Invalidation.html>

upvoted 2 times

🗲️ 👤 **PoCk3T** 8 months, 1 week ago

Just wanted to make sure you are aware this is a GCP certification here, not an AWS one.

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - B

upvoted 2 times

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

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

Correct Answers are (A) & (B):

A: Using VPC Flow Logs

VPC Flow Logs records a sample of network flows sent from and received by VM instances, including instances used as GKE nodes. These logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization.

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

(B): Firewall Rules Logging overview

Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules. For example, you can determine if a firewall rule designed to deny traffic is functioning as intended. Firewall Rules Logging is also useful if you need to determine how many connections are affected by a given firewall rule.

You enable Firewall Rules Logging individually for each firewall rule whose connections you need to log. Firewall Rules Logging is an option for any firewall rule, regardless of the action (allow or deny) or direction (ingress or egress) of the rule.

<https://cloud.google.com/vpc/docs/firewall-rules-logging>

upvoted 27 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : A and

upvoted 1 times

🗲️ 👤 **Arad** 1 month, 3 weeks ago

A & B are correct.

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

A and B

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - AB

upvoted 2 times

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

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

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.  
upvoted 15 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : D  
upvoted 1 times

🗲️ 👤 **Morgan91** 2 months, 3 weeks ago

D is correct  
upvoted 1 times

🗲️ 👤 **PeppaPig** 4 months, 1 week ago

GCP Implements Ingress using Global HTTP LB, it creates one Global LB for each Ingress object. So answer is D.  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is correct  
upvoted 1 times

🗲️ 👤 **namanp12345** 11 months ago

Correct Answer is (D)  
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D  
upvoted 1 times

🗲️ 👤 **Sysp** 1 year, 2 months ago

GKE ingress  
upvoted 3 times



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.

🗨️ 👤 **groovyorilla** Highly Voted 👍 1 year ago

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.

upvoted 6 times

🗨️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : A

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - A

upvoted 3 times

🗨️ 👤 **jonclem** 1 year, 2 months ago

A would appear to be correct as per the following link:  
<https://cloud.google.com/vpc/docs/using-vpc-peering>

upvoted 4 times

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

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

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/orelly/networking\\_2ndEd/fire/ch17\\_02.htm](https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch17_02.htm)

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

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

upvoted 11 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : D

upvoted 1 times

🗲️ 👤 **Arvinder** 7 months, 3 weeks ago

Correct answer is D

upvoted 1 times

🗲️ 👤 **pentium2000** 9 months, 2 weeks ago

D, only "Network TCP & UDP" LB supports UDP protocol.

upvoted 2 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is correct

upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D

upvoted 2 times

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

🗲️ 👤 **mozammil89** Highly Voted 👍 1 year, 10 months ago

The question asks for configuring internet-facing loadbalancer and not internal. Therefore correct answer should be "B".  
upvoted 25 times

🗲️ 👤 **architect** Highly Voted 👍 1 year, 6 months ago

This one is quite ambiguous, because we don't know much about the VoIP app.

A: No, VoIP is unlikely to use HTTP(S)

B: Likely - this is the only Internet-facing UDP option. VoIP apps tend to use UDP but we don't know that for sure.

C: No, has to be Internet facing

D: Maybe, if it does use TCP or SSL

upvoted 10 times

🗲️ 👤 **JohnnyBG** 5 months, 3 weeks ago

it's not ambiguous, TCP/SSL LB does not work on VoIP ports, only Internal/Network LB does.

upvoted 1 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks, 1 day ago

IMP - there are two answers: B&C... We don't know the actually design...but we know VOIP is best effort and is UDP...

Internal TCP/UDP Load Balancing distributes traffic among internal virtual machine (VM) instances IN the same region in a Virtual Private Cloud (VPC) network. It enables you to run and scale your services behind an INTERNAL IP address that is accessible ONLY to systems in the same VPC network or systems connected to your VPC network....

With that said - a Cloud Router is needed to connect from the Internet to hit the ILB...BUT a Global LB is need to distribute the traffic correctly so a NetworkLB is required. The design should be a Hub-n-Spoke or a Shared VPC with a Service VPC to hold the Cloud router and Network LB....

I will go with Answer b for now as in said INTERNET FACING VOIP Application.

Thoughts?

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks, 1 day ago

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

Check out the 3 tier diagram

upvoted 1 times

🗲️ 👤 **Tejtej** 2 weeks, 2 days ago

Selected Answer: 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

upvoted 1 times

🗲️ 👤 **Arad** 1 month, 3 weeks ago

B is correct.

upvoted 1 times

🗲️ 👤 **[Removed]** 8 months, 4 weeks ago

Assume the VOIP use UDP, then choose B.

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

B is the One

upvoted 1 times

🗨️ 👤 **ArizonaClassics** 10 months, 1 week ago

B is correct

upvoted 1 times

🗨️ 👤 **chetz12** 11 months, 2 weeks ago

I would go for A . HTTPS supports QUIC which can be used for VOIP

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

upvoted 3 times

🗨️ 👤 **cert1357** 1 year ago

I'll go with C. Use the flowchart.

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

upvoted 1 times

🗨️ 👤 **cert1357** 1 year ago

I mean B. Network Load Balancing

upvoted 1 times

🗨️ 👤 **Gharet** 1 year ago

I'm sorry but none of these answers seem likely, internal is not internet facing and the only one that google lists that supports UDP is the external facing TCP/UDP LB, if i just had to guess at one i would probably choose network load balancer but not sure how that could possibly be right either

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - B

upvoted 3 times

🗨️ 👤 **majun** 1 year, 2 months ago

C is the correct answer, A does not support, BD does not support internal balance

upvoted 1 times

🗨️ 👤 **jonclem** 1 year, 2 months ago

HTTP(S) LB has support for the QUIC protocol (VOIP). Therefore I'd go with A.

upvoted 2 times

🗨️ 👤 **[Removed]** 1 year, 4 months ago

UDP is used for VOIP applications because UDP ensures fast delivery of packets.

upvoted 3 times

🗨️ 👤 **passtest100** 1 year, 4 months ago

should be C. VoIP uses SIP protocol which is based on UDP. For internet access, in VOIP architecture, there is usually a SIP gateway which has public ip address to connect the internet, rather than the load balance. so C is the answer.

upvoted 2 times

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

🗨️ **rezavage** Highly Voted 1 year, 3 months ago

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.

upvoted 17 times

🗨️ **kumarp6** Most Recent 1 week, 1 day ago

Answer is : A

upvoted 1 times

🗨️ **desertlotus1211** 2 weeks, 1 day ago

The question is vague. It says 'between on-premise and GCP' BUT it doesn't tell you the direction - who is the source and who is the destination. It could either one! BUT this is a GCP test - why should we need to know about on-premise issues? [just being devil advocate].

Answer A seems 'more' right.

The likelihood GCP would need something from on-premise is possible - such as patches/updates/etc...

This is probably what the questions asking as well as in this video:

<https://www.youtube.com/watch?v=bmaarG0lkH8> Listen at about to 1min mark.

Answer is A...

upvoted 1 times

🗨️ **ASDF1467** 1 month, 4 weeks ago

Its A, <https://cloud.google.com/nat/docs/overview>

Cloud NAT allows outbound connections and the inbound responses to those connections. Each Cloud NAT gateway performs source NAT on egress, and destination NAT for established response packets.

Cloud NAT does not permit unsolicited inbound requests from the internet, even if firewall rules would otherwise permit

upvoted 1 times

🗨️ **EranSolstice** 2 months, 3 weeks ago

Cloud NAT (A) is only for outgoing connection so not the correct answer

If one want to allow your GCP instance to reach you on-premises network using say the internal IP of an instances as IP source you will need source NAT applied through iptables on that instances so (D) as well as some custom static route. However, that instances will also need to have ip\_forward enabled so (B) is also essential.

The question is ambiguous on which type of address translation will be performed, since it could also be achieved with DNAT (C). The only common element between those 2 options is ip forwarding, so I am going with (B). Pretty tricky.

upvoted 1 times

🗨️ **EranSolstice** 2 months, 3 weeks ago

I reread the question, correct answer is (A). When they refer to on-premies address block they refer to public IP of the on-premises network. Therefore (A) 200%.

upvoted 3 times

🗨️ **EranSolstice** 2 months, 3 weeks ago

For clarity, the question never mention that you have internal IP in GCP that want to talk to internal IP on your on-premises network. Many reader assume we have a VPN or interconnect link in the mix and that we want a solution to perform some advanced NAT between those network but it's not the case.

upvoted 2 times

🗨️ **jadson88888** 4 months, 2 weeks ago

When instances in on-prem Network needs to communicate with GCP, they can't use their private IP. They need a public IP instead. So it is source NAT that does the trick. Choose D.

upvoted 3 times

🗨️ **PiotrKam** 7 months ago

It's A, because: "Cloud NAT configures the Andromeda software that powers your Virtual Private Cloud (VPC) network so that it provides source network address translation (SNAT) for VMs without external IP addresses. Cloud NAT also provides destination network address translation

(DNAT) for established inbound response packets only."  
<https://cloud.google.com/nat/docs/overview#architecture>  
upvoted 2 times

  **jits1984** 4 months, 1 week ago

It also states that - "Cloud NAT does not implement unsolicited inbound connections from the internet. DNAT is only performed for packets that arrive as responses to outbound packets."

So C looks to me as the better option here.  
upvoted 2 times

  **Vidyasagar** 9 months, 3 weeks ago

A is the one  
upvoted 1 times

  **ArizonaClassics** 10 months, 1 week ago

my mistake the right Answer is A  
upvoted 1 times

  **ArizonaClassics** 10 months, 1 week ago


B is the right answer  
upvoted 1 times

  **groovyygorilla** 1 year ago



Likely C, but C & D are both possible.  
upvoted 1 times

  **noongooah** 1 year ago

its D. they want home router capabilities - src nat on prem blocks to connect to gcp  
upvoted 2 times

  **[Removed]** 1 year, 1 month ago

Ans - A  
upvoted 1 times

  **jfh6200** 1 year, 3 months ago

It's B  
upvoted 2 times

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.

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago  
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.

<https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#addkey>  
upvoted 13 times

🗲️ 👤 **kumarp6** Most Recent ⌵ 1 week, 1 day ago  
Answer is : A  
upvoted 1 times

🗲️ 👤 **Morgan91** 2 months, 3 weeks ago  
Correct Answer is (A)  
<https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys#edit-ssh-metadata>  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago  
A is the answer  
upvoted 1 times

🗲️ 👤 **ArizonaClassics** 10 months ago  
A is correct: @project level all instances in that project will access the ssh keys  
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - A  
upvoted 2 times

🗲️ 👤 **GANESH1985** 1 year ago  
@somabrataPani: can u please confirm that you have cleared ur gcp pcne exam using this site?  
upvoted 1 times

🗲️ 👤 **KWatHK** 11 months, 3 weeks ago  
I also think about A, because the question doesn't mention the security issues, and it mentioned that "every instance in your project" + "efficiently". If build a custom image, i don't think it is efficient.  
upvoted 1 times

🗲️ 👤 **majun** 1 year, 2 months ago  
I think the Correct answer is B. Project Metadata can be disabled when creating an instance.  
upvoted 1 times

🗲️ 👤 **majun** 1 year, 2 months ago  
as efficiently as possible , I think it should C, The premise is that the instances are created through mirroring.  
upvoted 1 times



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.

  **gless** Highly Voted 1 year ago

It is B for me:

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

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.

upvoted 12 times

  **desertlotus1211** Most Recent 2 weeks, 1 day ago

Answer is D.

This is a typical Arch. Design for shared VPC host project where you add your Security Appliance to control traffic between service projects [ E-W traffic]

upvoted 1 times

  **desertlotus1211** 2 weeks ago

Sorry, Answer D is incorrect... That answer says: ...Configure the appropriate routes to force traffic through to instance-A. Instance A is NOT the Security appliance.. unless its a typo, and it meant to say Instance B.

upvoted 1 times

  **matmuh** 1 month ago

Answer is D. We implement this scenario with palo-alto firewall. First of all you can't write a more specific route in the same vpc.

upvoted 2 times

  **desertlotus1211** 2 weeks ago

But Answer D shows the Instance A as the Security appliance, not Instance B...

The questions ask for traffic to go from Instance-A to Instance-B... Answer D has it the other way around...

upvoted 1 times

  **seddy** 8 months ago

The answer is 200 % D by elimination method.

1)It cannot be A or B because you are not allowed to create a more specific route than subnet route

2)You are not allowed to remove a subnet route. The only way to do so is by deleting the subnet itself.

Thus, by elimination the answer is D.

upvoted 2 times

  **densnoigaskogen** 7 months, 3 weeks ago

B should be the answer. It's question about defining static route.

The scenario is to require traffic from instance-A to be routed VIA instance-B in a different subnet, thus, instance-B's subnet is not the destination. "No other route can have a destination that matches or is more specific (has a longer subnet mask) than the destination of a subnet route." --> only applies when you try to set a destination CIDR within the subnet range. For example,if the 10.10.10.0/24 is the subnet, you can not define a static route which has destination ip range as 10.10.10.0/25.

When creating the static route for this question, you can select an instance (B) as next-hop, and use tag applied to instance-A to limit this static route to be only applicable for Instance-A.

upvoted 5 times

  **JoeShmoe** 7 months, 3 weeks ago

Agree. Its D for the reasons you give. Its a process of elimination question and in reality east west routing via firewall appliance would be across VPC's not subnet. Subnets are segreated by firewall rules not routes

upvoted 1 times

  **EranSolstice** 2 months, 3 weeks ago

Not sure, this is circular logic, after moving B to a different VPC, which route will you create to force routing of instance-A through instance-B without running into the same limitation of inability to define a more specific route then the system generated subnet route ?

Having security appliance that use multi-nic for east-west subnet isolation is a good pattern. But to achieve this you will need to move more then just instance-b to the other VPC.

upvoted 1 times

🗨️ 👤 **mwellger** 9 months, 1 week ago

For me the pertinent part of answer D that leads me to believe it's not the correct answer is "Configure the appropriate routes to force traffic through to instance-A." To me that suggests forcing the traffic from instance-b to instance-a, when in actual fact the question clearly stipulates that you want to force traffic from instance-a through instance-b

upvoted 1 times

🗨️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is the Correct answer

upvoted 2 times

🗨️ 👤 **ArizonaClassics** 10 months, 1 week ago

B is correct

upvoted 1 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - B

upvoted 2 times

🗨️ 👤 **rezavage** 1 year, 3 months ago

B is the best answer .Have the instance in another subnet should suffice to redirect the traffic by using specific route. No need to place the instance in another VPC . and you should have a tag to apply the route explicitly on the desired instance.

upvoted 3 times

🗨️ 👤 **iloveme** 1 year, 3 months ago

It's D. You can't have a more specific route

than a subnet route - <https://cloud.google.com/vpc/docs/routes#subnet-routes> - No other route can have a destination that matches or is more specific than the destination of a subnet route. You can create a custom route that has a broader destination range that contains the subnet route's destination range.

upvoted 5 times

🗨️ 👤 **eeghai7thioyaiR4** 10 months, 3 weeks ago

That is wrong (B is right)

"No other route can have a destination that matches or is more specific than the destination of a subnet route." does not apply here, because instance-b is not in the destination subnet

Also, you want subnet level isolation, so intra subnet flows are not supposed to pass through instance-b (no need to change that route)

upvoted 1 times

🗨️ 👤 **groovygorilla** 1 year ago

I agree. I think the answer is D.

upvoted 1 times

🗨️ 👤 **lukedj87** 1 year, 2 months ago

I think this is unrelated to subnet routes. The destination prefix in this case is 0.0.0.0/0. This does not match (or it's not even more specific) than subnet routes configured. So, I'd say B is the correct one.

upvoted 3 times

🗨️ 👤 **lukedj87** 1 year, 2 months ago

Sorry, I haven't paid attention to "more specific than subnet route". Then in this case it's for sure D.

upvoted 4 times

🗨️ 👤 **KWatHK** 11 months, 3 weeks ago

Static route with next-hop which could specify the instance or ip address. I think it should be what you are saying. more specify route than subnet route. so I will stay with B

upvoted 2 times

🗨️ 👤 **mozammil89** 1 year, 10 months ago

Configuring a VM as a NAT gateway

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

upvoted 2 times

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.

🗲️ 👤 **terrain** Highly Voted 👍 1 year, 5 months ago

"D" is correct  
<https://cloud.google.com/kubernetes-engine/docs/how-to/authorized-networks>  
upvoted 9 times

🗲️ 👤 **ThisisJohn** 2 months, 1 week ago

I believe the question means both the instance and the master are internal resources. If so, authorized network does not apply because

"Note: Authorized networks block untrusted IP addresses from outside Google Cloud. Addresses from inside Google Cloud (such as traffic from Compute Engine VMs) can reach your control plane using HTTPS, provided that they have the necessary Kubernetes credentials. "

<https://cloud.google.com/kubernetes-engine/docs/how-to/authorized-networks#overview>  
upvoted 2 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : D  
upvoted 1 times

🗲️ 👤 **walkwolf3** 3 weeks, 5 days ago

Answer is D.

Private clusters run nodes that only have internal IP addresses, and do not allow public IPs over the internet to access the control plane endpoint. Additionally, private clusters do not allow Google Cloud IP addresses to access the control plane endpoint by default. Using authorized networks in private clusters makes your control plane reachable only by allowed CIDRs, by nodes and Pods within your cluster's VPC, and by Google's internal production jobs that manage your control plane.

<https://cloud.google.com/kubernetes-engine/docs/how-to/authorized-networks>  
upvoted 1 times

🗲️ 👤 **qaz\_132** 3 months, 1 week ago

I will go with `D`. But this question is not very good. There are private cluster, public endpoint; private cluster, private endpoint. I believe they intened to ask for private cluster, private endpoint. If that is the case, then D for sure.  
upvoted 1 times

🗲️ 👤 **qaz\_132** 3 months, 1 week ago

I will go with `D`. But this question is not very good. There are private cluster, public endpoint; private cluster, private endpoint. I believe they intened to ask for private cluster, private endpoint. If that is the case, then D for sure.  
upvoted 1 times

🗲️ 👤 **PeppaPig** 3 months, 3 weeks ago

D 100%  
If you disable public endpoint access, then you must configure authorized networks for the private endpoint. If you don't do this, you can only connect to the private endpoint from cluster nodes or VMs in the same subnet as the cluster  
<https://cloud.google.com/kubernetes-engine/docs/concepts/private-cluster-concept#overview>  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is the one  
upvoted 4 times

🗲️ 👤 **ArizonaClassics** 10 months, 1 week ago

ans- D  
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D  
upvoted 2 times

🗲️ 👤 **saaurabh1805** 1 year, 4 months ago

D is correct answer here.

upvoted 2 times

  **maxth3mad** 1 year, 5 months ago

I think "D"

upvoted 2 times

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.

🗲️ 👤 **beebee** Highly Voted 👍 1 year, 5 months ago

Should be B: <https://cloud.google.com/compute/docs/access/iam>  
upvoted 11 times

🗲️ 👤 **terrain** Highly Voted 👍 1 year, 5 months ago

"B" should be the correct answer

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

"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."

upvoted 8 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : B  
upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks, 1 day ago

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

[roles/compute.networkAdmin](#)

.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.'

upvoted 1 times

🗲️ 👤 **buldas** 9 months ago

The answer is B:

[roles/compute.networkAdmin](#)

Permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates. The network admin role allows read-only access to firewall rules, SSL certificates, and instances (to view their ephemeral IP addresses). The network admin role does not allow a user to create, start, stop, or delete instances.

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

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

Correct Answer is B  
upvoted 1 times

🗲️ 👤 **pentium2000** 9 months, 3 weeks ago

Should be B,  
<https://cloud.google.com/compute/docs/access/iam#compute.networkAdmin>

[roles/compute.networkAdmin](#)

Permissions

compute.firewallPolicies.get

compute.firewallPolicies.list

compute.firewallPolicies.use

compute.firewalls.get

compute.firewalls.list

upvoted 2 times

🗲️ 👤 **cesar7816** 1 year, 1 month ago

B is correct, Network Admin role has permissions to list but not modify/delete firewall rules.  
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - B

upvoted 1 times

  **superpane** 1 year, 2 months ago

Definitely B.

The network admin role also grants the network team the ability to view but not modify firewall rules. <https://cloud.google.com/iam/docs/job-functions/networking>

upvoted 2 times

  **lukedj87** 1 year, 2 months ago

It's definitely C.

With the networkAdmin role only you cannot manage/view any firewall/ssl related config.

In order to achieve this, the only way is to create a custom role that gives full permissions on networking and the firewall list permission.

upvoted 2 times

  **saaurabh1805** 1 year, 4 months ago

B is correct answer here.

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

upvoted 1 times

  **HateMicrosoft** 1 year, 4 months ago

The correct answer is B.


This is a Shared VPC because "Your company has a security team that manages firewalls and SSL certificates."

So, Network Admins have full control over all network resources except for firewall rules and SSL certificates.

Network and Security Admins

[https://cloud.google.com/vpc/docs/shared-vpc#net\\_and\\_security\\_admins](https://cloud.google.com/vpc/docs/shared-vpc#net_and_security_admins)

upvoted 3 times

  **Jos** 1 year, 6 months ago

Should be C.

upvoted 4 times

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.

🗲️ 👤 **iobluedot** Highly Voted 👍 1 year, 4 months ago

C

[https://cloud.google.com/load-balancing/docs/health-check-concepts#content-based\\_health\\_checks](https://cloud.google.com/load-balancing/docs/health-check-concepts#content-based_health_checks)

upvoted 8 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks, 1 day ago

Answer is C: <https://cloud.google.com/load-balancing/docs/health-checks#optional-flags-hc-protocol-http>

<https://cloud.google.com/load-balancing/docs/health-checks>

Request path and Response: For HTTP, HTTPS, and HTTP2 protocols, you can optionally provide a URL path for the health check probe systems to contact.

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

C is correct

upvoted 2 times

🗲️ 👤 **marekmatula2020** 1 year, 1 month ago

B is correct. We have to configure the host header in health-check because as you know backend could host many domains and we have to know which one is a life.

upvoted 3 times

🗲️ 👤 **retep007** 3 months, 3 weeks ago

You can use http health check which does it for you

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 1 times

🗲️ 👤 **saaurabh1805** 1 year, 4 months ago

I will go with C

upvoted 2 times

🗲️ 👤 **beebee** 1 year, 5 months ago

Should be C

upvoted 2 times

🗲️ 👤 **maxth3mad** 1 year, 5 months ago

I think "C"

upvoted 2 times

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.

🗲️ 👤 **jonclem** Highly Voted 👍 1 year, 2 months ago

D is also incorrect. The question requires the "delete" permissions. The compute/networkAdmin role is the only one that offers this ability.  
upvoted 15 times

🗲️ 👤 **nikiwi** 1 year ago

you are right, D won't do  
upvoted 2 times

🗲️ 👤 **mozammil89** Highly Voted 👍 1 year, 10 months ago

The correct answer is "D", see this link below.

Permissions required for creating Interconnect VLAN attachment are following:

compute.interconnectAttachments.create  
compute.interconnectAttachments.get  
compute.routers.create  
compute.routers.get  
compute.routers.update

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

upvoted 11 times

🗲️ 👤 **sc00by** 9 months, 2 weeks ago

How can you delete the Interconnect VLAN attachments? In that list there are no permissions to modify or delete Interconnect VLAN attachments.  
upvoted 2 times

🗲️ 👤 **JohnnyBG** 5 months, 3 weeks ago

sc00by is right, it must be B because it has delete permission, see bellow from the console:

```
gcloud iam roles describe roles/compute.networkAdmin | grep inter
```

- compute.interconnectAttachments.create
- compute.interconnectAttachments.delete
- compute.interconnectAttachments.get
- compute.interconnectAttachments.list
- compute.interconnectAttachments.setLabels
- compute.interconnectAttachments.update
- compute.interconnectAttachments.use

upvoted 4 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : B  
upvoted 1 times

🗲️ 👤 **JesusMariaJose** 1 month, 3 weeks ago

Selected Answer: B

B - compute.networkAdmin had access to create, modify and delete vlans as you can see on link below: compute.interconnectAttachments.\*  
<https://cloud.google.com/compute/docs/access/iam#compute.networkAdmin>  
upvoted 1 times

🗲️ 👤 **JesusMariaJose** 1 month, 3 weeks ago

B is correct roles/compute.networkAdmin already has the permission to create, modify and delete vlan attachments.  
upvoted 1 times

🗲️ 👤 **seddy** 8 months ago

B is the answer  
upvoted 7 times

🗲️ 👤 **VivekMishraV** 8 months, 2 weeks ago



To perform this task, you must have been granted the following permissions or the following Identity and Access Management (IAM) roles.

















#### Permissions

compute.interconnectAttachments.create  
compute.interconnectAttachments.get  
compute.routers.create  
compute.routers.get  
compute.routers.update

#### Roles

roles/owner  
roles/editor  
roles/compute.networkAdmin

<https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/creating-vlan-attachments>  
upvoted 2 times

-   **CloudTrip** 9 months ago  
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.  
upvoted 3 times
-   **Vidyasagar** 9 months, 3 weeks ago  
D is right  
upvoted 1 times
-   **chetz12** 11 months, 2 weeks ago  
D is the correct answer as the ask is for least privileged access. NetworkAdmin will be an overkill for the task  
upvoted 1 times
-   **SGH93** 12 months ago  
B is correct  
upvoted 3 times
-   **ydanno** 1 year ago  
"B" is correct because we need a compute.interconnectAttachments.delete permission to delete VLAN attachments. The compute.networkAdmin role has it.  
upvoted 5 times
-   **[Removed]** 1 year, 1 month ago  
Ans - D  
upvoted 1 times
-   **saurabh1805** 1 year, 4 months ago  
If question is just for cloud interconnect delete, update and modofy then i will go for option C  
upvoted 1 times
-   **ravirajani** 1 year, 4 months ago  
During VLAN attachment creation, cloud router is also need modification. hence, all 5 permissions are required.  
hence, D  
[https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/creating-vlan-attachments#creating\\_vlan\\_attachments](https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/creating-vlan-attachments#creating_vlan_attachments)  
upvoted 1 times

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.

🗲️ 👤 **mozammil89** Highly Voted 👍 1 year, 10 months ago

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>  
upvoted 26 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : D  
upvoted 1 times

🗲️ 👤 **seddy** 7 months, 4 weeks ago

D for sure.  
Canary update is a rolling update type where you select a subset of instances to try the new features on. You gradually increase the # of instances to which the update applies on if all is well!

Peace :)  
upvoted 3 times

🗲️ 👤 **mwellger** 9 months, 2 weeks ago

A canary update is an update that is applied to a subset of instances in the group. With a canary update, you can test new features or upgrades on a random subset of instances, instead of rolling out a potentially disruptive update to all your instances. If an update is not going well, you only need to roll back the subset of instances, minimizing the disruption for your users.

Based on the above the answer for me would be D.  
upvoted 2 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

C is the answer  
upvoted 1 times

🗲️ 👤 **ArizonaClassics** 10 months ago

The Right Answer is D  
upvoted 1 times

🗲️ 👤 **ydanno** 1 year ago

"C" is correct.  
We perform a canary update if we have tested the new feature heavily.  
However, we have not tested heavily in this scenario.  
So we have to test the new feature and new template at first and have to MINIMIZE impacts to users.

There are some impacts on users if there are some bugs on its template and we test on a canary update.  
There is no impact on users if we test the new instances in the new instance group which is not provided to users.

So "D" has more impacts on users than "C".  
"C" is the least impactful way for users to test and update instances.  
upvoted 4 times

🗲️ 👤 **cesar7816** 1 year, 1 month ago

Ans is D, we need to use canary update in a current MIG, don't create a new one to test new version  
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D  
upvoted 2 times

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.

🗲️ 👤 **mozammil89** Highly Voted 👍 1 year, 10 months ago

Correct answer is A

upvoted 21 times

🗲️ 👤 **HateMicrosoft** 1 year, 4 months ago

<https://cloud.google.com/compute/docs/instance-groups/creating-groups-of-managed-instances>

upvoted 5 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : A

upvoted 1 times

🗲️ 👤 **seddy** 7 months, 4 weeks ago

Who posts these answers ahah! A for sure!

You can create a managed instance group in every region, but the statement does not require us to have that much availability! So creating a regional managed instance group in the existing region spanning over multiple zones should be enough!

Peace :)

upvoted 2 times

🗲️ 👤 **pentium2000** 9 months, 3 weeks ago

A is better answer.

B should go along with HTTP(S) Global Load Balancer. Otherwise, distributing traffic will be a painful process.

upvoted 1 times

🗲️ 👤 **cesar7816** 1 year, 1 month ago

I'll go with A

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - A

upvoted 1 times

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.

🗲️ 👤 **spidrfong** Highly Voted 👍 1 year, 2 months ago  
D is correct <https://cloud.google.com/cdn/docs/caching>  
upvoted 8 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago  
Answer is : D  
upvoted 1 times

🗲️ 👤 **kumarp6** 1 week, 1 day ago  
Answer is : D  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago  
D is correct  
upvoted 3 times

🗲️ 👤 **cesar7816** 1 year, 1 month ago  
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.  
upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - D  
upvoted 1 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago  
Should be D  
upvoted 3 times

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.

🗲️ 👤 **Vidyasagar** Highly Voted 👍 9 months, 3 weeks ago  
A is correct  
upvoted 8 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago  
Answer is : A  
upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks, 1 day ago  
If it's a gaming application - more than likely they're using a HTTPS LB  
upvoted 1 times

🗲️ 👤 **PeppaPig** 3 months, 3 weeks ago  
Really bad formed question, really ambiguous  
Is the traffic-scrubbing an external service, or one inside of your VPC?  
Is the global LB a HTTP LB or TCP/SSL on L4?  
As already pointed out by others, Cloud Armor only works together with global HTTP LB.  
upvoted 1 times

🗲️ 👤 **densnoigaskogen** 6 months, 1 week ago  
I would go with B.  
Cloud Armor can only be applied when using external HTTP(S) LB, not other global LBs. Additionally, Cloud Armor is placed between outside and your LB, which is inside GCP network, but outside your private VPC perimeter.  
The question says, it wants to restrict access to the origin, so, VPC Firewall rules are more applicable.  
upvoted 1 times

🗲️ 👤 **cesar7816** 1 year, 1 month ago  
Ans is A, Cloud Armor is used for LB, there is no way we can use FW rules at LB level  
upvoted 3 times

🗲️ 👤 **Hybrid\_Cloud\_boy** 1 year, 1 month ago  
Reading this leads me to believe A

The below links outlines NAT behavior of GCP global load balancer. Since this is a full proxy, the source IP of the scrubbing source would be translated to GFE IP, so allowing the scrubbing source via FW rule would not work.

So, by elimination this tells me that cloudarmor is the answer! So A

<https://cloud.google.com/load-balancing/docs/https>  
upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - A  
upvoted 1 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago  
I would go with A.  
Being able to use cloud armor really depends if the global LB is an HTTP LB (otherwise, cloud armor can't be used...)  
upvoted 3 times

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.

🗲️ 👤 **garbad** Highly Voted 👍 12 months ago  
Answer is A,

cost and complexity of multiple tunnel vpn is very high, also , dedicated interconnect is not required as required max speed is 1.5gbps  
Also , direct connectivity is bogus verb, all the solution provide direct connectivity to your vpc instance , once connected through router  
upvoted 11 times

🗲️ 👤 **[Removed]** Highly Voted 👍 1 year, 1 month ago  
Ans - C  
upvoted 6 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago  
Answer is : A  
upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks ago  
<https://cloud.google.com/blog/products/networking/google-cloud-network-connectivity-options-explained>  
Answer A is better...  
upvoted 1 times

🗲️ 👤 **MrPajonko** 2 weeks, 4 days ago  
Selected Answer: C  
It states that private RFC 1918 ip addressing is required. Partner Interconnect doesn't use private IP addressing, public only. Correct answer is C.  
upvoted 2 times

🗲️ 👤 **desertlotus1211** 2 weeks ago  
You need to revisit how Partner and Dedicated Interconnect works...Public IPs are only needed for BGP peering  
upvoted 1 times

🗲️ 👤 **MrPajonko** 2 weeks ago  
Sorry guys for misleading - Pricate Interconect ofcourse use private IP addressing.  
upvoted 1 times

🗲️ 👤 **ThisisJohn** 2 months, 1 week ago  
I would vote for A because of this statement " Most of the data transfer will be from GCP to the on-premises environment."  
  
According to the documentation, carrier peering "Has reduced internet egress rates to your on-premises network " while Cloud VPN "Has standard egress rates for traffic sent through an Interconnect connection;" <https://cloud.google.com/network-connectivity/docs/how-to/choose-product#cp-compare>  
upvoted 3 times

🗲️ 👤 **JohnnyBG** 5 months, 3 weeks ago  
Everybody that says C please do not take this exam and never be consulted for network related question ...  
upvoted 4 times

🗲️ 👤 **jeeet\_** 6 months, 2 weeks ago  
C,  
Question is challenging.  
--> application can burst upto 1.5Gbps,  
--> Cloud VPN- can burst upto 3Gbps, and with double VPN we can minimize packet loss and bandwidth upto 6Gbps,

-> Interconnect initial setup is complex, you need to email to google, then talk to your vendor (which is google itself) and common peer zone. It's time consuming.

Since they already have a single tunnel VPN, setting up another won't take much of time.

upvoted 1 times

  **seddy** 7 months, 4 weeks ago

C for sure!

Key elements: 1) Direct Connectivity (cannot be partner inter)

2) Cannot be Dedicated bc we want low cost

3) Multiple VPN tunnels with ECMP will help us deal with packet losses

Peace :)

upvoted 1 times

  **cloudy** 2 months ago

partner interconnect is a direct connectivity

upvoted 1 times

  **JohnnyBG** 6 months ago

Partner interconnect IS a direct connectivity ..

upvoted 3 times

  **buldas** 9 months ago

Unless we know how much data will be transferred, we really can not give an answer.

Because at some point (about 45-50TB) Interconnect will get cheaper then VPN.

But knowing that this app can get a burs 1,5 Gbps, and we sure can think that his state stays longer than 30 minutes. The answer I would give is A.

upvoted 2 times

  **CloudTrip** 9 months ago

I think Answer will be A as 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.

upvoted 1 times

  **pentium2000** 9 months, 3 weeks ago

I'll go A,

C is too painful to find tune routing. In addition, as a network engineer, I don't wanna get trouble replying on a internet link with packets loss.

upvoted 2 times

  **chetz12** 11 months, 1 week ago

A strong proponent of C

<https://www.noction.com/blog/equal-cost-multipath-ecmp>

upvoted 1 times

  **DrAnney** 1 year ago

The question says direct connectivity to instances on GCP. Therefore, C in the best answer. The VPN will connect directly to the GCP instances

A - partner is not direct connectivity from on-prem to GCP instances



B - The is costly and the question says solution has to be cost effective.

upvoted 2 times

  **Gharet** 1 year ago

Shouldn't it be A? I would think the complexity of multiple tunnels and ECMP (not sure that matter's in VPN) be complex? Plus maybe all the egress charges over the internet, i think i would go with A here.

upvoted 1 times

  **majun** 1 year, 2 months ago

Cost and the complexity of the solution should be minimal , It should be C

upvoted 1 times



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 caused autoscaling to reach the maximum number of instances, and users of your application cannot complete transactions. After an investigation, you think it as a DDOS attack. You want to quickly restore user access to your application and allow successful transactions while minimizing cost. Which two steps should you take? (Choose two.)

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

🗨️ **Hybrid\_Cloud\_boy** Highly Voted 1 year, 1 month ago

I think B,E are actually correct.

A and C would increase cost to global LB, change app architecture, and could potential block legitimate traffic since you “think” it is a DDoS, but do i not know. I do not think google would recommend blocking traffic unless you KNOW.

So a temp increase in auto scale, with further investigation is the best course of action. It may lead to some short-term cost increase, but ultimately less cost increase than moving to global LB premium tier with cloudarmor.

upvoted 11 times

🗨️ **Alex\_74** Highly Voted 4 months, 3 weeks ago

A & C

Cloud Armor is the solution to prevent and mitigate attack (DDOS SQL injection and so on), it's a revenue generating so have to be alive and protected.

No Cloud Armor is not a firewall. Using the CA language you have tons of prebuild rules to evaluate and block the malicious traffic in automatic way. You can put the rule blocking a specific traffic but it's not there the value (you have the firewall for that).

Than you need C cause Cloud Armor require an HTTP(s) load balancer (that can be used cause it's a web application)

upvoted 7 times

🗨️ **walkwolf3** 3 weeks, 5 days ago

This would be a long term solution if DDOS is confirmed. The quickest solution is to recover the service, which is BE.

upvoted 1 times

🗨️ **Windy\_Welly88** 1 month, 2 weeks ago

I'd go A & C. These days you can get Cloud Armor for trial, and this product will mitigate current AND sustained DDOS attacks. Would you REALLY autoscale for a massive DDOS attack, do you think Google will let you do this for free? You wont need to spend time looking at logs and traffic as it will tell you straight away who the actors are.. And finally, since this is a critical revenue-earning application any downtime would be a significant cost. Only way to ensure uptime would be to use Cloud Armor.

upvoted 1 times

🗨️ **kumarp6** Most Recent 1 week, 1 day ago

Answer is : B and E

upvoted 1 times

🗨️ **desertlotus1211** 2 weeks, 1 day ago

What about A&B? Since an investigations is done to reveal 'maybe' a DDoS attack - you may now the IP Source... We don't know the metrics that is used for autoscaling... is it CPU or some other metric? We can go back to the autoscaling policy and increase the max number of instances... This is quick and dirty until we know for sure on what is causing the autoscaling max limit to be reached...

Thoughts?

upvoted 1 times

🗨️ **lollo883** 3 months ago

I think B,C are correct:

Cloud armor is not supported in network LB so A cant be possible. Moreover, D cant be because of the downtime of the service. E is just useless in this scenario.

With B we rely on the DDOS mitigation system of GCP infrastructure (From the documentation we have "Even without a Google Cloud Armor configuration, Google infrastructure and GFEs provide defense-in-depth for DDOS attacks and SYN floods."). C is the only way to restore the service immediatly.

upvoted 3 times

🗨️ **PeppaPig** 4 months ago



Answer is B, C. Keep in mind that DDoS protection is auto-on for HTTP Load Balancer.

B is obvious, because scaling out can quickly mitigate the issue.

For C, DDoS protection is provided by default if you use HTTP, TCP and SSL LB even without Cloud Armor configuration

"All projects that include HTTP(S) Load Balancing, TCP Proxy Load Balancing, or SSL Proxy Load Balancing are automatically enrolled in Google Cloud Armor Standard"

[https://cloud.google.com/armor/docs/managed-protection-overview#standard\\_versus\\_plus](https://cloud.google.com/armor/docs/managed-protection-overview#standard_versus_plus)

"Even without a Google Cloud Armor configuration, Google infrastructure and GFEs provide defense-in-depth for DDoS attacks and SYN floods."



[https://cloud.google.com/load-balancing/docs/https#open\\_ports](https://cloud.google.com/load-balancing/docs/https#open_ports)

upvoted 3 times

  **ExamTopicsFan** 4 months, 1 week ago



Assume for a second that it was a real DoDOD attack .Only option A can prevent it from happening again or stop it if it in progress . None of the other options can do it. So Option A is a must.

upvoted 3 times

  **Zuy01** 4 months, 2 weeks ago

the key is quick and minimizing cost here, i think the ans is BE

upvoted 2 times

  **jeeet\_** 6 months, 2 weeks ago

Quickly restore user access--

B and E makes sense,

1. with just B, you'll be able to help users to access your application. (as they are already using Network LB- that has highest bandwidth available -> meaning low congestion)

E. Since now you let your application work again, Now quickly getting the nature of DDOS attack can help mitigate the issue further, Like knowing those IP's you can block them using Firewalls etc.

upvoted 2 times

  **seddy** 7 months, 4 weeks ago

A and C where you first use preview-mode in Cloud Armor to make sure!

upvoted 3 times

  **seddy** 7 months, 4 weeks ago


Also, not in the answers but, since this is a NW LB, which is a pass through, we could actually create firewall rules to prevent the traffic from the source if we knew the source IP. Using firewall rules to prevent traffic is not possible for proxy based LB'ers but it's possible for NW LB as it is a pass through! This is the least costly option. But we do need to know the IP address of the traffic!

upvoted 1 times

  **CloudTrip** 8 months, 3 weeks ago

No changing the LB doesn't take as much as time than analysing issues through a Putty (SSH) login and going through tons from logs. This is from practical experience and still going with B,C as the most practical response in situations like this which also goes inline with the question statement.

upvoted 1 times

  **WakandaF** 8 months, 3 weeks ago



B & E? are correct?

upvoted 2 times

  **CloudTrip** 9 months ago


The key requirement is here "quickly restore user access to your application and allow successful transactions while minimizing cost" which makes B,C as the right choice. E is going to be time consuming and A needs you to setup Cloud Armor which also has high price tag based on your usage. Operationally think in day to day scenario, it's B, C what you can do immediately restore access and without spending much.

upvoted 1 times

  **buldas** 8 months, 4 weeks ago

Changing the load balancer will take time too.

upvoted 2 times

  **Vidyasagar** 9 months, 3 weeks ago


A and C

upvoted 2 times

  **ArizonaClassics** 10 months ago

Ans= B&E (provides you quick and temporal fix and no additional costs)

upvoted 2 times

  **LaXuS** 10 months, 3 weeks ago

I think B&E is correct. It says "You want to quickly restore user access to your application and allow successful transactions while minimizing cost." if you want to quickly restore access you need temp increase in auto scale while your figuring out the cause of the sudden burst of traffic.

upvoted 3 times

  **chetz12** 11 months, 2 weeks ago

AC as B&D can't be a cost-effective solution as well as it doesn't help with identifying the origin of the attack. E can't be viable as you have to think of what's next.

upvoted 1 times

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.

  **mlyu** Highly Voted 1 year, 2 months ago

Answer are A & C

C is definitely correct. private services access require private connection

In below links stated Service Networking API is required

<https://cloud.google.com/service-infrastructure/docs/enabling-private-services-access>

upvoted 18 times

  **Alex\_74** 4 months, 3 weeks ago

A & C

<https://cloud.google.com/sql/docs/mysql/private-ip>

This page provides information about using private IP with Cloud SQL. For step-by-step instructions for configuring a Cloud SQL instance to use private IP, see Configuring private IP.

upvoted 3 times

  **ESP\_SAP** Highly Voted 1 year, 2 months ago

Correct Answer are (C) & (E):

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](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>

upvoted 8 times

  **VivekMishraV** 8 months, 1 week ago

For Accessing K8S and Cloud SQL it is Google Private Service Access

upvoted 3 times

  **kumarp6** Most Recent 1 week, 1 day ago

Answer is : A and C

upvoted 1 times

  **kumarp6** 1 week, 2 days ago

A & C


[https://cloud.google.com/sql/docs/mysql/private-ip#network\\_issues](https://cloud.google.com/sql/docs/mysql/private-ip#network_issues)

upvoted 1 times

  **Arad** 1 month, 3 weeks ago

A & E are correct.

upvoted 1 times

  **Arad** 1 month, 3 weeks ago

Correction: A & C.

upvoted 1 times























  **ThisisJohn** 2 months ago

D & E

E because "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>

D because "Your network must have appropriate routes for the destination IP ranges used by Google APIs and services. These routes must use the default internet gateway next hop" <https://cloud.google.com/vpc/docs/configure-private-google-access#requirements>

upvoted 1 times

-   **PeppaPig** 4 months, 1 week ago  
A&C are correct.  
Private Google Access is for connecting to the standard Google public APIs. Cloud SQL is NOT a public API  
upvoted 1 times
-   **PeppaPig** 4 months, 1 week ago  
Cloud SQL under the hood is just a VM instance managed by Google that runs in a Google managed VPC  
upvoted 1 times
-   **cyma** 6 months, 3 weeks ago  
A,C,E all works. but, for E, it use VM's internal IP to connect to Cloud SQL's external IP. My English is not good. If 'without public IP' means for the VM instances. then A/C/E works. if 'without public IP' means for Cloud SQL, then only A/C works.  
upvoted 1 times
-   **CloudTrip** 9 months ago  
Answer will be B, E as you need Private Google Access for API scenarios like this. <https://cloud.google.com/vpc/docs/configure-private-google-access> and also you need to enable the API services <https://cloud.google.com/vpc/docs/access-apis-external-ip#requirements>  
upvoted 1 times
-   **Vidyasagar** 9 months, 3 weeks ago  
C and E  
upvoted 1 times
-   **chetz12** 11 months, 2 weeks ago  
C & E  
<https://cloud.google.com/sql/docs/mysql/configure-private-ip>  
upvoted 2 times
-   **chetz12** 11 months, 2 weeks ago  
Not exactly.... A & C makes more sense now  
upvoted 3 times
-   **cesar7816** 1 year, 1 month ago  
Agree A and C  
  
Service Networking enables you to offer your managed services on internal IP addresses to service consumers. Service consumers use private services access to privately connect to your service  
upvoted 3 times
-   **[Removed]** 1 year, 1 month ago  
Ans - AC  
upvoted 4 times
-   **majun** 1 year, 2 months ago  
it should be C&E  
upvoted 1 times
-   **lukedj87** 1 year, 2 months ago  
Agree with A and C.  
  
E is completely unrelated. Private Google Access is only for services not backed up by some GCE instances  
upvoted 4 times

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

🗲️ 👤 **porsak** Highly Voted 👍 11 months ago

The answer is D.

<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.

upvoted 15 times

🗲️ 👤 **ArizonaClassics** Highly Voted 👍 10 months, 2 weeks ago

The answer is D: Partner interconnect is of two types layer 2 and layer 3

With Layer 2 Interconnect you MUST configure BGP on your on-prem router

With Layer 3: router configuration and peers are fully automated.

Hence the question "Your on-prem router cannot run a BGP protocol configuration"

upvoted 5 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : D

upvoted 1 times

🗲️ 👤 **Gharet** 1 year ago

D is the answer - For layer 2 connections, you must configure and establish a BGP session between your Cloud Routers and on-premises routers for each VLAN attachment that you create. The BGP configuration information is provided by the VLAN attachment after your service provider has configured it. For a Layer 3 connection BGP is configured from your partner to the Cloud Router in GCP, no need for BGP on-premise.

upvoted 3 times

🗲️ 👤 **cesar7816** 1 year, 1 month ago

I'll go with C, BGP is layer 4 but in this case it use Layer 3

Essentially, the carrier provides a Layer 3 Partner Interconnect service to you, and then "binds" your VLAN attachment with the correct MPLS VPN on the carrier's edge device. Because this is a Layer 3 service model, the BGP session is established between your Cloud Router and your VRF inside the carrier edge device.

upvoted 1 times

🗲️ 👤 **iqbalangga** 1 year, 1 month ago

Absolutely D

upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D

upvoted 2 times

🗲️ 👤 **majun** 1 year, 2 months ago

it should be D, layer 2 partner need local route BGP, layer 3 not need , so answer is D

upvoted 2 times

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`

🗲️ 👤 **kumarp6** 1 week, 1 day ago

Answer is : B

upvoted 1 times

🗲️ 👤 **Arad** 1 month, 3 weeks ago

B is correct.

upvoted 1 times

🗲️ 👤 **PeppaPig** 4 months ago

B Easy :))

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

B is the one

upvoted 4 times

🗲️ 👤 **sindra** 1 year ago

confirm B <https://cloud.google.com/vpc/docs/add-remove-network-tags>

upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - B

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

upvoted 2 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago

Correct answer is B

upvoted 2 times

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

Which next hop should you choose?

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

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

Correct Answer is (C):

When you create a route based tunnel using the Cloud Console, Classic VPN performs both of the following tasks:

Sets the tunnel's local and remote traffic selectors to any IP address (0.0.0.0/0)

For each range in Remote network IP ranges, Google Cloud creates a custom static route whose destination (prefix) is the range's CIDR, and whose next hop is the tunnel.

<https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns>

upvoted 8 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **EranSolstice** 2 months, 3 weeks ago

Likely C. The gcloud certainly support that parameter. <https://cloud.google.com/sdk/gcloud/reference/compute/routes/create>

Worth to mention that this apply only for the "classic VPN" product that will be phased out in March 2022. HA VPN cannot be referenced that way ( they do not support static route, BGP only ).

upvoted 2 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

C is correct

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 1 times

🗲️ 👤 **majun** 1 year, 1 month ago

C is Correct

upvoted 1 times

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.

🗲️ 👤 **ydanno** Highly Voted 👍 1 year ago

"D" is correct.

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>

upvoted 9 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : D

upvoted 1 times

🗲️ 👤 **Arad** 1 month, 3 weeks ago

D is correct.

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is right

upvoted 4 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D

upvoted 3 times

🗲️ 👤 **majun** 1 year, 1 month ago

Cloud CDN leverages Google Cloud global external HTTP(S) load balancers to provide routing, health checking, and Anycast IP support.

Because global external HTTP(S) load balancers can have multiple backend instance types— Compute Engine VM instances, Google Kubernetes Engine Pods, Cloud Storage buckets, or external origins outside of Google Cloud—you can choose which backends (origins) to enable Cloud CDN for.

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

upvoted 2 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago

Should be D

upvoted 3 times



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.



  **ESP\_SAP** Highly Voted 1 year, 2 months ago  
Correct Answer is (A):



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>  
upvoted 12 times



  **narangikhatmal** 11 months, 3 weeks ago  
why not D,there is no constraint avoiding \*/video  
upvoted 2 times



  **lukedj87** 1 year, 2 months ago  
Agree with A. Thanks for the link!  
upvoted 1 times

  **kumarp6** Most Recent 1 week, 1 day ago  
Answer is : A  
upvoted 1 times

  **seddy** 8 months ago  
200% A  
For those who claim it's D, I assure you it is not. The reason is that you can only use a '\*' at the end of a path rule followed by a '/'. So a path rule consisting of a '\*' MUST end like '...../\*' and that's the rule!  
upvoted 2 times

  **Vidyasagar** 9 months, 3 weeks ago  
A is right  
upvoted 1 times

  **eeghai7thioyaiR4** 10 months, 3 weeks ago  
I would go with D  
  
There is probably a lot of links everywhere, so rearranging the directory structure may not be easy  
  
With D, you do not change any of the code, SEO is left unaffected too, and you can map the old paths to the right buckets  
upvoted 3 times

  **[Removed]** 1 year, 1 month ago  
Ans - A

upvoted 1 times

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

Which connection type should you choose?

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

🗲️ 👤 **majun** Highly Voted 👍 1 year, 1 month ago

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

<https://cloud.google.com/network-connectivity/docs/direct-peering>

upvoted 6 times

🗲️ 👤 **Windy\_Welly88** 1 month, 2 weeks ago

Yes, question says using a public IP address, which you would use with Direct Peering. I don't believe you need a public address for dedicated interconnect?

upvoted 1 times

🗲️ 👤 **majun** 1 year, 1 month ago

Answer Should be B

upvoted 3 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : B

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks ago

Answer is B: Direct Peering

<https://cloud.google.com/network-connectivity/docs/direct-peering>

'When established, Direct Peering provides a direct path from your on-premises network to Google services, including Google Cloud products that can be exposed through one or more public IP addresses'

The next section is misleading: 'Direct Peering exists outside of Google Cloud. Unless you need to access Google Workspace applications, the recommended methods of access to Google Cloud are Dedicated Interconnect or Partner Interconnect.'

BUT we're not accessing Google Cloud and in the questions is says 'connection to Google'. Direct Peering allows access to the Google Cloud service we need - Cloud SQL via Public IP.

Thoughts?

upvoted 1 times

🗲️ 👤 **LisX** 3 months, 3 weeks ago

C. Direct Peering exists outside of Google Cloud. Unless you need to access Google Workspace applications, the recommended methods of access to Google Cloud are Dedicated Interconnect or Partner Interconnect.

upvoted 3 times

🗲️ 👤 **desertlotus1211** 2 weeks ago

When established, Direct Peering provides a direct path from your on-premises network to Google services, including Google Cloud products that can be exposed through one or more public IP addresses...Google Cloud Products... Cloud SQL is a Google Cloud Product.

You're not accessing a Google Cloud... only a service in it.

upvoted 1 times

🗲️ 👤 **ThisisJohn** 2 months ago

Agree with you also because you can use Private Google Access from on-prem to access Cloud SQL as per the below:

(Cloud Interconnect) "Does not give you access to Google Workspace, but gives you access to all other Google Cloud products and services from your on-premises network. Also allows access to supported APIs and services by using Private Google Access from on-premises hosts."

<https://cloud.google.com/network-connectivity/docs/how-to/choose-product#dp-compare>


upvoted 1 times

🗲️ 👤 **jeeet\_** 6 months, 2 weeks ago

why dedicated interconnect or partner interconnect is the answer?

it's because they are dependent of third party service provider and Google is itself for Dedicated internconnect.

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Ans - B

upvoted 4 times

  **lukedj87** 1 year, 2 months ago

I'd go with B

upvoted 2 times

Question #62

Topic 1

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

Where should you create the Cloud Router instance?

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

  **Vidyasagar** Highly Voted  9 months, 3 weeks ago

C is correct

upvoted 5 times

  **kumarp6** Most Recent  1 week, 1 day ago

Answer is : C

upvoted 1 times

  **cesar7816** 1 year, 1 month ago

yes, C no doubt, we need to configure it in the Host project

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 1 times

  **hjson821109** 1 year, 2 months ago

Agree with C

upvoted 1 times

  **lukedj87** 1 year, 2 months ago

I think it's C

upvoted 1 times

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.

  **lukedj87** Highly Voted  1 year, 2 months ago



C for sure. Since it's a new VPC, all other ingress traffic is automatically denied by default  
upvoted 6 times

  **kumarp6** Most Recent  1 week, 1 day ago

Answer is : C  
upvoted 1 times

  **bike123** 9 months, 1 week ago

C is correct  
upvoted 3 times

  **Vidyasagar** 9 months, 3 weeks ago

C is correct  
upvoted 2 times

  **[Removed]** 1 year, 1 month ago

Ans - C  
upvoted 2 times

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

During troubleshooting you find:

"ç Each on-premises router is configured with the same 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 The VPN logs have no-proposal-chosen lines when the VPNs are connecting.

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

What is the most likely cause of this problem?

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

  **ArizonaClassics** Highly Voted  10 months ago

I will go with A

Reason:

If the VPN logs show a no-proposal-chosen error, this error indicates that Cloud VPN and your peer VPN gateway were unable to agree on a set of ciphers. For IKEv1, the set of ciphers must match exactly. For IKEv2, there must be at least one common cipher proposed by each gateway. Make sure that you use supported ciphers to configure your peer VPN gateway.

<https://cloud.google.com/network-connectivity/docs/vpn/support/troubleshooting#:~:text=If%20the%20VPN%20logs%20show,of%20ciphers%20must%20match%20exactly.&text=Make%20sure%20that%20you%20use,configure%20your%20peer%20VPN%20gateway.>

upvoted 11 times

  **kumarp6** Most Recent  1 week, 1 day ago

Answer is : A

upvoted 1 times

  **danzcamacho** 1 week, 2 days ago

right option is B, for the table in this link [https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster\\_sizing\\_secondary\\_range\\_pods](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster_sizing_secondary_range_pods)

upvoted 1 times

  **desertlotus1211** 2 weeks ago

Answer is A: <https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies>

This seems to be a case for classic VPN. The BGP session is not established because the VPN session is not configured correctly. LBs are not needed...

Thoughts?

upvoted 1 times

  **JesusMariaJose** 1 month, 3 weeks ago

Selected Answer: A



A is answer

upvoted 1 times

  **pentium2000** 9 months, 3 weeks ago



I'll go A, only A makes sense in this situation.

upvoted 2 times

  **Vidyasagar** 9 months, 3 weeks ago

Correct one C

upvoted 1 times

  **Ocedoc** 11 months, 2 weeks ago

I'm going with D here. Lack of load balancer isn't preventing one of the BGP sessions from establishing. The second BGP session not being established is preventing load balancing to the alternate vpn.


As far as the wording of D, (BGP sessions are NOT established between BOTH on-premises routers and ...) think of it this way: Not both, only one. If only one of your eyes can see, then you cannot see with both eyes.

upvoted 1 times

  **yhl** 1 year ago

A is right. VPN did tunnel didn't work.

upvoted 4 times

  **JonP24** 1 year ago

A is correct - as it needs to match the proposals for the VPN to establish

B - firewall rules dont have any effect on establishing IPSec VPNs using Cloud VPN

C - Load balancer is not in the picture here since this is a Cloud VPN peering

D - for the BGP session to reach an established state, the IPSec session must come up first.

upvoted 3 times

  **Gharet** 1 year ago

Correct Answer A - The VPN logs have no-proposal-chosen lines when the VPNs are connecting indicates to me the VPN is not established hence BGP would not come up.

upvoted 3 times

  **Hybrid\_Cloud\_boy** 1 year, 1 month ago

Actually - Ignore me. I think it is A

D says “both” which is wrong - But if the tunnel is down, that would explain why BGP is not established.

So I choose A

upvoted 3 times

  **Hybrid\_Cloud\_boy** 1 year, 1 month ago

Interesting - I’ve agreed w. ESP\_SAP a lot, but this one I don’t understand his logic.

I’m going with D actually.... it spells out that BGP is not established?

This BGP issue would explain why ECMP is not taking both paths

upvoted 1 times

  **Hybrid\_Cloud\_boy** 1 year, 1 month ago

Actually - A is right. Down VPN would explain down BGP neighbor. And unlike D, A only refers to 1 connection.

upvoted 2 times

  **[Removed]** 1 year, 1 month ago

Ans - B

(Confused)

upvoted 2 times

  **ESP\_SAP** 1 year, 2 months ago

Correct Answer (C):

Part 2

After packets are delivered to the VPC network, the internal load balancer distributes them to backend VMs according to the configured session affinity.

If the lb-network has two routes, each with the destination 192.168.1.0/24 and a next hop corresponding to different VPN tunnels, responses from backend VMs can be delivered over each tunnel according to the priority of the routes in the network. If different route priorities are used, one tunnel can serve as a backup for the other. If the same priorities are used, responses are delivered by using ECMP.

Replies sent from the backend VMs (such as vm-a2) are delivered directly to the on-premises clients through the appropriate tunnel.

From the perspective of lb-network, if routes or VPN tunnels change, traffic might egress by using a different tunnel. This might result in TCP session resets if an in-progress connection is interrupted.

<https://cloud.google.com/load-balancing/docs/l7-internal/internal-https-lb-and-other-networks>


upvoted 1 times

  **lukedj87** 1 year, 2 months ago

I don't agree. LBs, interconnect and VLANs are IMHO totally unrelated here.

I think the key point here is that one of the two routers doesn't even form the BGP peering session, meaning that likely port 179 is blocked. So I'd go with B

upvoted 2 times

  **ESP\_SAP** 1 year, 2 months ago

Correct Answer is (C):

Part 1:

You must configure each tunnel or each Cloud Interconnect attachment (VLAN) in the same region as the internal load balancer (unless, for Internal TCP/UDP Load Balancing, you've enabled global access). Multiple tunnels or VLANs can provide additional bandwidth or can serve as standby paths for redundancy.

Keep in mind the following points:

If the on-premises network has two routes with the same priorities, each with a destination of 10.1.2.0/24 and a next hop corresponding to a different VPN tunnel in the same region as the internal load balancer, traffic can be sent from the on-premises network (192.168.1.0/24) to the load balancer by using equal-cost multipath (ECMP).

upvoted 1 times



You need to define an address plan for a future new GKE cluster in your VPC. This will be a VPC native cluster, and the default Pod IP range allocation will be used. You must pre-provision all the needed VPC subnets and their respective IP address ranges before cluster creation. The cluster will initially have a single node, but it will be scaled to a maximum of three nodes if necessary. You want to allocate the minimum number of Pod IP addresses.

Which subnet mask should you use for the Pod IP address range?

A. /21

B. /22

C. /23

D. /25

  **groovygorilla** Highly Voted 1 year ago

I think it's B.

"This will be a VPC native cluster, and the \*default\* Pod IP range allocation will be used."

From <https://cloud.google.com/kubernetes-engine/docs/how-to/flexible-pod-cidr#overview>

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

That is, /24 for one node.

We have 3 nodes, so we need /22.

upvoted 17 times

  **lukedj87** Highly Voted 1 year, 2 months ago

TL;DR: correct answer /22

Max nodes will be three.

Each node can have a max of 254 pods.

$254 * 3 \rightarrow 762$  pods

Both a /25 and /23 wouldn't be enough --> those would respectively account for 128 and 512 pods

/21 would be too large -> that would be enough for 2048 pods

/22 is the right one, accounting for 1024 PODs

upvoted 9 times

  **lollo883** 3 months, 3 weeks ago

In GKE the maximum number of pods per node is hard limited to 110. So in this question we have to estimate 330 pods. Anyway, GKE has an ultraconservative policy on IP addresses number, so for every pod 2 IP addresses are reserved (even if only one is actually assigned).

So we have 330 pods, we double this number  $330 * 2 = 660$  and we get the minimum number of IP addresses we need. So 512 aren't enough and we go with 1024. To reserve 1024 IP addresses ( $2^{10}$ ) we need to use a /22 subnet

upvoted 3 times

  **kumarp6** Most Recent 1 week, 1 day ago

Answer is : B

upvoted 1 times

  **kumarp6** 1 week, 1 day ago

Answer is : B

upvoted 1 times

  **kumarp6** 1 week, 2 days ago

it's B

[https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#defaults\\_limits](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#defaults_limits)

upvoted 1 times


  **JesusMariaJose** 1 month, 3 weeks ago

Selected Answer: B

B

[https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#defaults\\_limits](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#defaults_limits)

upvoted 1 times

  **Morgan91** 3 months, 1 week ago


[https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster\\_sizing\\_secondary\\_range\\_pods](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster_sizing_secondary_range_pods)

upvoted 1 times

  **vamgcp** 3 months, 2 weeks ago

Correction to my below reply - Each node will have max of  $2^8 = 256$ , so for 3 nodes it will be  $256 * 3 = 768$ . If you chose /23 then  $2^{(32-23)} = 2^9 = 512$  which is less than 768 so incorrect option .if you do the same thing for /22 you get 2048 which is more than 768 hence option B /22 is correct

upvoted 1 times

  **vamgcp** 3 months, 2 weeks ago

Each node will have max of  $2^8 = 254$ , so for 3 nodes it will be  $254 * 3 = 762$ . If you chose /23 then  $2^{(32-23)} = 2^9 = 512$  which is less than 762 so incorrect option .if you do same thing for /212 you get 2048 which is more than 762 hence option B /21 is correct

upvoted 1 times

  **PeppaPig** 4 months, 1 week ago

B is the answer.

When the "default" Pod IP range allocation is used, GKE assigns /24 CIDR block for pods on each node, which means the minimum secondary IP range of the subnet is /24, and that allows for max 1 node in your cluster.

To expand to 3 Nodes, /22 range is required.

upvoted 1 times

  **PeppaPig** 4 months, 1 week ago

Calculate the maximum number of nodes, N, that the subnet's secondary IP address range for Pods can support:

$N = 2^{(M - S)}$  where:

M is the size of the netmask of each node's alias IP address range for Pods, calculated in the first step

S is the size of the subnet mask of the subnet's secondary IP address range

[https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster\\_sizing\\_secondary\\_range\\_pods](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster_sizing_secondary_range_pods)



upvoted 1 times

  **PiotrKam** 6 months, 4 weeks ago

It's C - /23



[https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster\\_sizing](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#cluster_sizing)

upvoted 3 times

  **Vidyasagar** 9 months, 3 weeks ago



C is correct

upvoted 3 times

  **LaXuS** 10 months, 3 weeks ago

I think B is the right answer. although best practice suits the answer C I will go with B because it says "it will scaled to a maximum of three nodes if necessary" so there's a chance you will not be using all of the ip address and if t scales to a maximum you can still accomodate it with the minimum number of ip addresses

upvoted 3 times

  **LaXuS** 10 months, 3 weeks ago

oops i switched the B and C. C is the right choice

upvoted 1 times



  **porsak** 11 months ago

I think it's a tricky question. You can't have just three nodes, just 2 or 4. Default Pod IP range will be used so /24. For 4 nodes with 110 pods for each node u have to allocate /22 IPs. Also if you use their equation ( $24 - 22 = 2$ ,  $2^2 = 4$  nodes). 1024 addresses.

See: <https://cloud.google.com/kubernetes-engine/docs/how-to/flexible-pod-cidr>

[https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#defaults\\_limits](https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips#defaults_limits)

upvoted 1 times

  **[Removed]** 8 months, 3 weeks ago

you can have 3 nodes

upvoted 1 times

  **chetz12** 11 months, 2 weeks ago

I would go with /23 as it says minimum IP addresses to fulfill the total of  $110 * 3 = 330$  which is  $> /24$  (256) and less than the next best option which is /23 (512)

upvoted 1 times

  **chetz12** 11 months, 2 weeks ago

Correct is C /22 . Forgot the fun part around the best practice and it's mentioned in one of the thread here.

upvoted 1 times

  **ydanno** 1 year ago

"D" is correct.

We want to allocate the minimum number of Pod IP addresses so we use /25 for Pod IP adressess.

<https://cloud.google.com/kubernetes-engine/docs/how-to/flexible-pod-cidr#overview>

upvoted 3 times

  **glk** 1 year ago

D should the answer as it says "You want to allocate the minimum number of Pod IP addresses"

upvoted 2 times

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.

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

Correct Answer is (D):

Firewall Rules Logging has the following specifications:

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>

upvoted 17 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago

Agree!

upvoted 1 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : D

upvoted 1 times

🗲️ 👤 **kumarp6** 1 week, 2 days ago

Answer is D

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is correct

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D

upvoted 3 times

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

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

  **mikelabs** Highly Voted 1 year, 2 months ago

Answer is B & D.

B: Minimizes cost and quickly.

D: You need to create firewall rules to allow traffic between subnets over each VPC.

upvoted 10 times

  **seddy** Highly Voted 8 months ago

B and D 100%

-First of all, we only have 2 separate VPCs in 2 different projects each where each project resides in the same organization. This set-up already yells that we need NW peering!

-In addition, to be able to use a Shared VPC we need to delete existing service project resources and recreate them in the shared VPC subnet, which is something the question statement does not want, so Shared VPC is automatically eliminated

-Lastly, with nw peering, the subnet routes of both VPCs are automatically shared, but we still need to create firewall rules to allow incoming requests for both ends.

Hence B and D

upvoted 7 times

  **kumarp6** Most Recent 1 week, 1 day ago

Answer is : B and D

upvoted 1 times

  **kumarp6** 1 week, 2 days ago

Answer is B & D.

upvoted 1 times

  **VivekMishraV** 8 months, 1 week ago

it B and D

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

When you connect networks using VPC Network Peering, firewall rules are not exchanged between them. To allow ingress traffic from VM instances in a peer network, you must create ingress allow firewall rules. By default, ingress traffic to VMs is blocked by the implied deny ingress rule.

If you need to restrict access to VMs such that only other VMs in your VPC network have access, ensure that the sources for your ingress allow firewall rules only identify VMs in your VPC network, not ones from peer networks. For example, you can specify source IP ranges for just the subnets in your VPC network.

To restrict access to an internal TCP/UDP load balancer, create ingress firewall rules that apply to the load balancer's backend VMs.



upvoted 5 times

  **Plinci** 9 months ago

Has to be A and B.


D would not work as VPCs are in different projects, allowing all traffic would expose resources on it externally, you can't allow the subnet private ranges as it would reach the VPC with an external IP through Internet and not the source subnet private IP ranges.

upvoted 1 times

  **buldas** 8 months, 4 weeks ago

VPN or Peereing, A and B doesn't make any sense.

upvoted 1 times

  **Vidyasagar** 9 months, 3 weeks ago

B and D

upvoted 4 times


  **subhala** 1 year ago

How about A and B?

upvoted 1 times

  **cesar7816** 1 year, 1 month ago

B and D,  
upvoted 2 times

  **[Removed]** 1 year, 1 month ago

Ans - BD  
upvoted 2 times

  **lukedj87** 1 year, 2 months ago

I'm sure about B, not that sure about D...but it's the only other option -by exclusion- that makes sense to me  
upvoted 2 times

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

- ☞ IP ranges for pods and services must be as small as possible.
- ☞ The nodes and the master must not be reachable from the internet.
- ☞ You must be able to use kubectl commands from on-premises subnets to manage the cluster.

How should you create the GKE cluster?

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

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago  
Correct Answer is (D):

Creating GKE private clusters with network proxies for controller access

When you create a GKE private cluster with a private cluster controller endpoint, the cluster's controller node is inaccessible from the public internet, but it needs to be accessible for administration.

By default, clusters can access the controller through its private endpoint, and authorized networks can be defined within the VPC network.

To access the controller from on-premises or another VPC network, however, requires additional steps. This is because the VPC network that hosts the controller is owned by Google and cannot be accessed from resources connected through another VPC network peering connection, Cloud VPN or Cloud Interconnect.

<https://cloud.google.com/solutions/creating-kubernetes-engine-private-clusters-with-net-proxies>

upvoted 13 times

🗲️ 👤 **JohnnyBG** 5 months, 1 week ago

All that document is saying is that you need to export your route to Google's VPC where the master is. Private endpoint is not required .. I would go with C on this one.

upvoted 2 times

🗲️ 👤 **JohnnyBG** 5 months, 1 week ago

scratch that .. the peering between Google's VPC is done via a private endpoint .. D is OK I guess

upvoted 1 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago

Agree with D

upvoted 1 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : D

upvoted 1 times

🗲️ 👤 **kumarp6** 1 week, 2 days ago

Answer is : D

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

D is correct

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - D

upvoted 1 times

You are creating an instance group and need to create a new health check for HTTP(s) load balancing.

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

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

🗲️ 👤 **densnoigaskogen** Highly Voted 👍 7 months ago

A and C.

Unless you use target pool-based Network LB, then it's required to use legacy health check, otherwise, legacy health check is not recommended to be used for HTTP(S) LB.

ref: <https://cloud.google.com/load-balancing/docs/health-check-concepts>

upvoted 7 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : A and C

upvoted 1 times

🗲️ 👤 **kumarp6** 1 week, 2 days ago

Answer is A&C

upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 week, 6 days ago

This one is tricky!

Answers are A&C...

Though you can create a legacy health check for HTTP(S) load balancing via gcloud tools -however it's ONLY for Target Pools, not instance groups. look here:

<https://cloud.google.com/load-balancing/docs/health-check-concepts>

And also - the question is not referring to an HTTP(S) Load Balancer...it's referring to HTTP(S) load Balancing.

Also when they are referring to 'new' health check - they imply to the NEW instance group. so selecting an existing HC is feasible since it's 'new' to the instance group... ;)

Thoughts?

upvoted 1 times

🗲️ 👤 **PeppaPig** 3 months, 3 weeks ago

Answer is A&C

Legacy health check is only applicable and required when you use target pool based NLB.

For almost all other load balancer types, you MUST use regular, non-legacy health checks where the protocol matches the load balancer's backend service protocol.

[https://cloud.google.com/load-balancing/docs/health-check-concepts#category\\_and\\_protocol](https://cloud.google.com/load-balancing/docs/health-check-concepts#category_and_protocol)

upvoted 2 times

🗲️ 👤 **seddy** 8 months ago

A and C for sure!

Link: <https://cloud.google.com/load-balancing/docs/health-checks>

-Important lines from the link that lead me to say the answer is A and C:

"Google Cloud allows you to create or select a health check when you complete the load balancer's backend configuration in the Cloud Console." - A

"You can create a health check using the Cloud Console, the gcloud command-line tool, or the REST APIs." - C

Peace :)

upvoted 4 times

🗲️ 👤 **[Removed]** 8 months, 3 weeks ago

I support AD, legacy can not use console. [https://cloud.google.com/load-balancing/docs/health-checks#console\\_4](https://cloud.google.com/load-balancing/docs/health-checks#console_4)

upvoted 2 times

🗲️ 👤 **CloudTrip** 9 months ago

Answer is A,C as "Traffic Director and most load balancers use non-legacy health checks, but target pool-based Network Load Balancing requires that you use legacy health check". This question asks about https load balancer so definitely C makes a better choice than E.

upvoted 1 times



🗨️ 👤 **Vidyasagar** 9 months, 3 weeks ago

A and C

upvoted 1 times

🗨️ 👤 **mamh** 10 months ago

Although the Cloud Console's health checks page lists and allows you to edit both health checks and legacy health checks, you cannot create a new legacy health check from the Cloud Console's health checks page.

AD

To create a legacy health check, use the Cloud Console's network load balancer page or use this section's gcloud or API instructions.

<https://cloud.google.com/load-balancing/docs/health-checks#legacy-health-checks>

upvoted 1 times

🗨️ 👤 **eeghai7thioyaiR4** 10 months, 2 weeks ago

Why not B: health checks are in the "instance groups" section, not the "vpc network" one

Why not C: you want to create a new check, so selecting an existing one is not an option

Why not E: you cannot create legacy health check using the GCP console

So at the end:

- can you create a check via gcloud: yes

- can you create a legacy check via gcloud: yes too

Both the "current" and the "legacy" health checks can be used for http load balancing

-> A and D

upvoted 2 times

🗨️ 👤 **glk** 1 year ago

I think its AC: Although the Cloud Console's health checks page lists and allows you to edit both health checks and legacy health checks, you cannot create a new legacy health check from the Cloud Console's health checks page.

To create a legacy health check, use the Cloud Console's network load balancer page or use this section's gcloud or API instructions.

<https://cloud.google.com/load-balancing/docs/health-checks#create-legacy-health-checks>

upvoted 3 times

🗨️ 👤 **[Removed]** 1 year, 1 month ago

Ans - AC

upvoted 1 times

🗨️ 👤 **lukedj87** 1 year, 2 months ago

It's A and C

upvoted 1 times

🗨️ 👤 **marekmatula2020** 1 year, 2 months ago

The question is about the HTTP(S) load balancer so the A and C are correct.

upvoted 4 times



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

Which connectivity method should you choose?

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

🗲️ 👤 **kumarp6** 1 week, 1 day ago  
Answer is : A  
upvoted 1 times

🗲️ 👤 **kumarp6** 1 week, 2 days ago  
A is correct  
upvoted 1 times

🗲️ 👤 **desertlotus1211** 1 week, 6 days ago  
<https://cloud.google.com/network-connectivity/docs/vpn/pricing>  
  
Cloud VPN \$0.050 Hourly charge for each tunnel attached to the gateway  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago  
A is correct  
upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - A  
upvoted 2 times

🗲️ 👤 **hjson821109** 1 year, 2 months ago  
A is correct  
upvoted 3 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago  
definitely, A  
upvoted 4 times

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

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

🗲️ 👤 **marekmatula2020** Highly Voted 👍 1 year, 2 months ago  
C is correct. A is incorrect because in on-prem is not BGP router  
upvoted 6 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago  
Answer is : C  
upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago  
C is correct  
upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - C  
upvoted 1 times

🗲️ 👤 **hjson821109** 1 year, 2 months ago  
It should be C  
upvoted 1 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago  
I'd go with C, specifying the local subnets to be used for the SAs in the tunnel  
upvoted 1 times

🗲️ 👤 **superpane** 1 year, 2 months ago  
you do not have a device capable of speaking Border Gateway Protocol (BGP). it can't be A. I'd say C  
upvoted 1 times

🗲️ 👤 **superpane** 1 year, 2 months ago  
"you do not have a device capable of speaking Border Gateway Protocol (BGP)". It can be A. I should say C  
upvoted 1 times

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.

🗲️ 👤 **LY** Highly Voted 👍 11 months, 2 weeks ago

Answers are A and E. A is very clear.

Both C and E look OK per <https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring>

But, this question is about "find data about how the request are being distributed", so, E is the right answer as it is monitoring backend\_request\_count

upvoted 13 times

🗲️ 👤 **kumarp6** Most Recent ⌵ 1 week, 1 day ago

Answer is : A and C

upvoted 1 times

🗲️ 👤 **densnoigaskogen** 7 months ago

I would choose A and C.

A - is obvious and easiest way to see the traffic distribution to the backend instances.

D - On Stackdriver Monitoring console, Monitoring metrics for Load balancer already include a list of pre-defined metrics, e.g Backend request count, thus, there is no need to create new dashboard and metric, thus E is NOT correct.

Ref: [https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring#viewing\\_dashboards](https://cloud.google.com/load-balancing/docs/https/https-logging-monitoring#viewing_dashboards)

upvoted 2 times

🗲️ 👤 **densnoigaskogen** 7 months ago

typo, I meant A and D.

upvoted 3 times

🗲️ 👤 **CloudTrip** 9 months ago

I think the answer will be A,E as https/backend\_request\_count will provide the "The number of requests sent from the external HTTP(S) load balancer to the backends" which is requested in the question about how the distribution is done to the backend.

upvoted 3 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

A and D

upvoted 2 times

🗲️ 👤 **1973cat** 12 months ago

I think its a A and C

upvoted 1 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - AD

upvoted 1 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago

I think it's A D but it would be great having someone reinforcing (or not!) my answer..

upvoted 2 times

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

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

🗲️ 👤 **ESP\_SAP** Highly Voted 👍 1 year, 2 months ago

Correct Answer is (C):

Provisioning overview

Start by connecting your on-premises network to a supported service provider. Work with the service provider to establish connectivity.

Next, create a VLAN attachment for a Partner Interconnect in your GCP project. This generates a unique pairing key that you'll use to request a connection from your service provider. You'll also need to provide other information such as the connection location and capacity.

After the service provider configures your attachment, activate it to start using it. For more information about the provisioning process, see the Provisioning Overview in the Partner Interconnect how-to guide.

[https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview#provisioning\\_overview](https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview#provisioning_overview)

upvoted 16 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks ago

Answer is C

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks ago

1. o create and provision a Partner Interconnect connection, follow these steps:

Create a VLAN attachment

Create a VLAN attachment for a Partner Interconnect connection. This step generates a pairing key that you share with your service provider. The pairing key is a unique key that lets a service provider identify and connect to your Virtual Private Cloud (VPC) network and associated Cloud Router. The service provider requires this key to complete the configuration of your VLAN attachment.

upvoted 1 times

🗲️ 👤 **seddy** 8 months ago

The answer is definitely C.

-It cannot be B because our selected service provide already has an established connectivity between their resources and Google edge point in a Google colocation facility.

-The very first thing in Partner interconnect is to establish connectivity between our on-prem nw and the service provider edge point. This should be done first! Service provider already needs to have a connection to Google edge point in Google's colocation

-Then, we create a VLAN attachment in Cloud console and send the pairing key to our provider in order for them to establish connectivity from their resources to our selected VPC network (a Vlan is always associated with a specific VPC)

Thus the answer is C.

Peace :)

upvoted 1 times

🗲️ 👤 **ArizonaClassics** 10 months, 2 weeks ago

Here is the Google recommended steps for provisioning partner interconnect

1. Create a VLAN
2. Request a connection from service provider
3. Activate connection with a VLAN attachment
4. Configure BGP

Hence the question says "You already have a service provider".\Therefore that eliminates step 1. Now your next step is .....Answer is B

upvoted 2 times

🗲️ 👤 **porsak** 11 months ago

I think D is the right answer. Because YOU ALREADY HAVE AN INTERCONNECT PARTNER and you want to use it. You just need to pre-activate or directly activate the connection.

You must activate it before the attachment can start passing traffic.

A: nonsense

B: Interconnect partner already have a physical connection.

C: I already have Interconnect partner  
D: right answer - need to activate the connection.  
<https://cloud.google.com/network-connectivity/docs/interconnect/how-to/partner/activating-connections#gcloud>  
<https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview>  
upvoted 1 times

- ydanno** 1 year ago

"B" is correct. First of all, we have to do provision a connection.  
  
<https://cloud.google.com/network-connectivity/docs/interconnect/concepts/partner-overview?hl=En#provisioning>  
"To provision a Partner Interconnect connection with a service provider, you start by connecting your on-premises network to a supported service provider. Work with the service provider to establish connectivity.  
  
Next, you create a VLAN attachment for a Partner Interconnect connection in your Google Cloud project, which generates a unique pairing key that you use to request a connection from your service provider. "  
upvoted 1 times
- [Removed]** 1 year, 1 month ago

Ans - C  
upvoted 1 times
- lukedj87** 1 year, 2 months ago

It's C for sure  
upvoted 1 times

Question #74

Topic 1

You need to centralize the Identity and Access Management permissions and email distribution for the WebServices Team as efficiently as possible.  
What should you do?

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

- [Removed]**

Highly Voted

1 year, 1 month ago

Ans - A  
upvoted 6 times
- kumarp6**

Most Recent

1 week, 1 day ago

Answer is : A  
upvoted 1 times
- EranSolstice** 2 months, 3 weeks ago

I think it's (B). Otherwise (A) will not help at all in regards to centralize email distribution. E.g. a Cloud Identity "group" by itself as per (A) is just an identity, you can assign permission and member to it but you cannot send email to it. It's just a group, unless you have an already existing workgroup with MX pointing to it.  
upvoted 1 times
- EranSolstice** 2 months, 3 weeks ago

On second though, it's likely (A). It would be very unusual to create a workgroup and cloud identity domain just for one team. Usually workgroup are enterprise wide.  
upvoted 1 times
- lukedj87** 1 year, 2 months ago

I would create a group, so A  
upvoted 2 times
- mikelabs** 1 year, 2 months ago

That's correct. But you must assume that you have a G Suite account, because you need distribute emails too.  
upvoted 1 times

You are using the gcloud command line tool to create a new custom role in a project by copying a predefined role. You receive this error message: INVALID\_ARGUMENT: Permission resourcemanager.projects.list is not valid

What should you do?

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

🗲️ 👤 **cesar7816** Highly Voted 👍 1 year, 1 month ago

Agree C, if you try doing the same you will get this

These permissions can only be added to custom roles at the organization level; they have no effect at the project level or below.

resourcemanager.projects.list

upvoted 5 times

🗲️ 👤 **kumarp6** Most Recent 🕒 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **desertlotus1211** 2 weeks ago

Answer is C:

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

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

C is correct

upvoted 3 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 2 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago

It's C. If you try from the console, you'll see that that role is not applicable to project-level custom roles

upvoted 3 times

One instance in your VPC is configured to run with a private IP address only. You want to ensure that even if this instance is deleted, its current private IP address will not be automatically assigned to a different instance.

In the GCP Console, what should you do?

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

🗲️ 👤 **seddy** Highly Voted 👍 8 months ago

it's C!

You cannot change the internal IP address of an existing VM. You can do that for an external IP tho! The only way to preserve a VM's existing internal IP is by upgrading it to a static IP!

Peace :)

upvoted 7 times

🗲️ 👤 **kumarp6** Most Recent ⌚ 1 week, 1 day ago

Answer is : C

upvoted 1 times

🗲️ 👤 **ExamTopicsFan** 3 months, 2 weeks ago

C

<https://cloud.google.com/compute/docs/ip-addresses/reserve-static-internal-ip-address#promote-in-use-internal-address>

If you have ephemeral IP addresses that are currently in use, you can promote these addresses to static internal IP addresses so the addresses remain with your project until you actively remove them.

upvoted 1 times

🗲️ 👤 **Vidyasagar** 9 months, 3 weeks ago

C is correct

upvoted 2 times

🗲️ 👤 **ydanno** 1 year ago

"C" is correct.

Because in this scenario, we have a RUNNING instance and ensure that the current private IP address is a static address. We cannot change the internal IP address of an existing instance. "B" is wrong.

On the other hand, we can promote the ephemeral internal IP address of a resource to a static internal IP address. "C" is correct.

upvoted 4 times

🗲️ 👤 **nikiwi** 1 year ago

definitely C, this is tested working

upvoted 2 times

🗲️ 👤 **gless** 1 year, 1 month ago

If we go with theory...

I would chose answer C --> <https://cloud.google.com/compute/docs/ip-addresses/reserve-static-internal-ip-address#reservenewip>

Since here <https://cloud.google.com/compute/docs/ip-addresses/reserve-static-internal-ip-address#reservenewip> it is written that "automatically allocated or an unused address from an existing subnet".

upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 2 times

🗲️ 👤 **mikelabs** 1 year, 2 months ago

Answer is C, because you need the current internal IP and not another IP.

upvoted 3 times

🗲️ 👤 **hjson821109** 1 year, 2 months ago

Definately B

upvoted 1 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago

Here <https://cloud.google.com/compute/docs/ip-addresses/reserve-static-internal-ip-address#restrictions>, this is mentioned:

You cannot change the internal IP address of an existing resource. For example, you cannot assign a new static internal IP address to a running VM instance. You can, however, promote the ephemeral internal IP address of a resource to a static internal IP so that the address remains reserved even after the resource is deleted.

upvoted 1 times

  **lukedj87** 1 year, 2 months ago

....anyway, after trying multiple times from the console, I don't find a way to achieve this, so I'm start thinking that B might be a better option

upvoted 1 times

  **lukedj87** 1 year, 2 months ago

For sure, C

upvoted 3 times



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.

🗲️ 👤 **superpane** Highly Voted 👍 1 year, 2 months ago  
Sorry, correct is B, the more specific takes priority  
upvoted 11 times

🗲️ 👤 **mikelabs** 1 year, 2 months ago  
I agree with you  
upvoted 2 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago  
Agree! Apologise. I made confusion between answers. B is correct  
upvoted 2 times

🗲️ 👤 **kumarp6** Most Recent ⌵ 1 week, 1 day ago  
Answer is : B  
upvoted 1 times

🗲️ 👤 **Morgan91** 3 months ago  
B si correct answer.  
<https://cloud.google.com/vpc/docs/routes#routeselection>  
upvoted 1 times

🗲️ 👤 **pentium2000** 9 months, 2 weeks ago  
The answer is B,  
Here is the routing table after the maintenance job  
10.1.0.0/16 -> directly connected route  
10.2.0.0/16 -> directly connected route  
10.3..1.0/24 -> directly connected route  
10.0.0.0/8 -> next hop is on-prem

As you can see, routing is go "longest matched" method, so instance see 10.2.1.25 as a local network device. Solution

1. On-prem should announce more specific route rather than /8.
  2. The theory of design the network is wired, why do you add a overlapping subnet on your vpc.
- upvoted 2 times

🗲️ 👤 **[Removed]** 1 year, 1 month ago  
Ans - B  
upvoted 3 times

🗲️ 👤 **superpane** 1 year, 2 months ago  
The on-prem router announces 10/8.  
But that cannot be reached because subnet routes (more specific than 10/8) are getting prioritized over route coming from the VPN, so the DB can't be reached.  
So in that case is A, the problem is caused the more specific routes take priority  
upvoted 3 times

🗲️ 👤 **lukedj87** 1 year, 2 months ago  
The answer is A.  
The on-prem router announces 10/8.  
But that cannot be reached because subnet routes (more specific than 10/8) are getting prioritized over route coming from the VPN, so the DB can't be reached.  
upvoted 2 times

🗲️ 👤 **hjson821109** 1 year, 2 months ago  
I agree with A  
upvoted 1 times

  **lukedj87** 1 year, 2 months ago

Sorry, my comment was correct. But the answer is B. Local subnet VPC routes are MORE specific!

upvoted 4 times

  **Jasonwcc** 1 year, 2 months ago

Since router is advertising 10.0.0.0/8 that includes all the 3 subnets. Then I don't see how A,B,C is denying that. D is the answer

upvoted 3 times

Question #78

Topic 1

You need to create a new VPC network that allows instances to have IP addresses in both the 10.1.1.0/24 network and the 172.16.45.0/24 network.

What should you do?

- A. Configure global load balancing to point 172.16.45.0/24 to the correct instance.
- B. Create unique DNS records for each service that sends traffic to the desired IP address.
- C. Configure an alias-IP range of 172.16.45.0/24 on the virtual instances within the VPC subnet of 10.1.1.0/24.
- D. Use VPC peering to allow traffic to route between the 10.1.0.0/24 network and the 172.16.45.0/24 network.

  **Jasonwcc** Highly Voted  1 year, 2 months ago



Should be C. Primary range with secondary range then assign as aliases to vNIC

upvoted 7 times

  **kumarp6** Most Recent  1 week, 1 day ago

Answer is : C



upvoted 1 times

  **Ethanra** 1 month, 2 weeks ago

Selected Answer: C

C is correct

upvoted 1 times

  **Vidyasagar** 9 months, 3 weeks ago

C is correct

upvoted 1 times

  **[Removed]** 1 year, 1 month ago

Ans - C

upvoted 1 times

  **hjson821109** 1 year, 2 months ago

I agree with C

upvoted 1 times

  **lukedj87** 1 year, 2 months ago

Definitely, C

upvoted 1 times

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

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

🗨️  **seddy** Highly Voted 👍 8 months ago

Im pretty sure if this was an exam question then the expected answer would be B (NW load balancer)

1) the question says external TCP which is either TCP proxy or Network LB.


2) The question does NOT state anything about LB being regional or global, so there is no harm in choosing Network Load balancer instead of TCP proxy

3) TCP proxy is not a pass through LB, but network LB is. So, Network LB preserves the client IP by default.

NOTE: It is still possible to preserve the client IP via TCP proxy if you use a Proxy Protocol. So, if the question statement was "External GLOBAL Tcp LB" then i would say the answer is TCP Proxy. But with all we have in the statement, Network LB is a safe answer!

Peace :)

upvoted 6 times

🗨️  **seddy** 7 months, 4 weeks ago

I was wrong, the question indeed says Global. So the answer is D. We cannot preserve the client IPs by default. To do that we need to use a Proxy Protocol.

upvoted 8 times

🗨️  **EranSolstice** 2 months, 3 weeks ago

The question refer to a "global load balancer \*solutions\*". If you create an NLB in multiple region and pair it with an adequate cloud DNS that is region based this may be considered a global load balancer solution.

upvoted 1 times

🗨️  **EranSolstice** 2 months, 3 weeks ago

I take that back. D is the way.

upvoted 1 times

🗨️  **EranSolstice** 2 months, 3 weeks ago

I agree with your original analysis. Ans is B

upvoted 1 times

🗨️  **EranSolstice** 2 months, 3 weeks ago

I take that back. Proxy protocol can allow (D) to reserve the original source IP/port <https://cloud.google.com/load-balancing/docs/tcp/setting-up-tcp#proxy-protocol>

upvoted 1 times

🗨️  **ydanno** Highly Voted 👍 1 year ago

You can understand which LB we should use in this situation. The correct answer is "D".

External -> no SSL offload -> Global LB -> TCP Proxy

[https://cloud.google.com/load-balancing/docs/choosing-load-balancer#flow\\_chart](https://cloud.google.com/load-balancing/docs/choosing-load-balancer#flow_chart)

There is one important point to note.

By default, the original(source) client IP address and port information is not preserved. We can preserve this information by using the PROXY protocol.

<https://cloud.google.com/load-balancing/docs/tcp#target-proxies>

upvoted 5 times

🗨️  **coffeecupz** Most Recent ☹️ 1 day, 18 hours ago

Are these questions updates as of 01/01/2022?

Can someone confirm please?

upvoted 1 times

🗨️  **kumarp6** 1 week, 1 day ago

Answer is : D































upvoted 2 times

🗨️  **desertlotus1211** 2 weeks ago

Answer is D:

<https://medium.com/google-cloud/preserving-client-ips-through-google-clouds-global-tcp-and-ssl-proxy-load-balancers-3697d76feeb1>

upvoted 2 times

-   **asd1010** 1 month, 1 week ago  
Preserving client source IP addresses  
To preserve the original source IP addresses of incoming connections to the load balancer, you can configure the load balancer to prepend a PROXY protocol version 1 header to retain the original connection information. For more information, see [Update proxy protocol header for the proxy](#).  
Answer : D  
<https://cloud.google.com/load-balancing/docs/ssl>  
upvoted 2 times
-   **PeppaPig** 4 months ago  
D is the answer.  
You need to enable PROXY prototol to retain client source IP  
<https://cloud.google.com/load-balancing/docs/tcp/setting-up-tcp#proxy-protocol>  
upvoted 3 times
-   **network\_020** 7 months, 2 weeks ago  
B is the correct answer. Reference - <https://cloud.google.com/load-balancing/images/choose-lb.svg>  
upvoted 2 times
-   **WakandaF** 8 months, 3 weeks ago  
D - <https://medium.com/google-cloud/preserving-client-ips-through-google-clouds-global-tcp-and-ssl-proxy-load-balancers-3697d76feeb1>  
upvoted 4 times
-   **Plinci** 9 months ago  
I would say D.  
This one it's a bit tricky. Since it's "global external TCP load balancing solution":  
- Not A (asks for a TCP LB).  
- it can't be B (Network LB it's regional).  
- Neither C (needs to be external LB).  
  
By default TCP/SSL proxy load balancer original client IP address and port information is not preserved, but it can be preserved using the PROXY protocol:  
<https://cloud.google.com/load-balancing/docs/tcp#target-proxies>  
upvoted 4 times
-   **Vidyasagar** 9 months, 3 weeks ago  
D is correct  
upvoted 2 times
-   **arielp** 10 months, 4 weeks ago  
Rather confused with the option, if B.. that is not global.. only regional.. if choose D.. does not preserve ip address....  
upvoted 2 times
-   **chetz12** 11 months, 2 weeks ago  
Lol this one is a check and mate: D is my answer  
upvoted 2 times
-   **GANESH1985** 1 year ago  
Answer is B, go to use cases on this page:<https://cloud.google.com/load-balancing/docs/network>  
upvoted 2 times
-   **GANESH1985** 1 year ago  
Can anyone please confirm that you have passed the exam using the answers from the discussions?  
upvoted 1 times
-   **sleekdunga** 8 months, 3 weeks ago  
Instead of seeking confirmation, why don't you do your due diligence by studying and contributing your response here with reference urls? By the way the Answer here is D. The term global rules out B and you can preserve client IP using option D.  
upvoted 3 times
-   **[Removed]** 1 year, 1 month ago  
Ans - D  
upvoted 5 times
-   **hjson821109** 1 year, 2 months ago  
Answer is B  
upvoted 1 times
-   **lukedj87** 1 year, 2 months ago  
Network load balancers are regional, not global.  
upvoted 3 times
-   **Rodine** 8 months ago  
But in question isn't mentioned that it has to be global, IT HAS TO BE EXTERNAL, so Network is external LB and additionally preserve IP address to the backend which TCP Proxy doesn't.  
upvoted 1 times

