

🔗 Google Discussions



## Exam Professional Cloud Security Engineer All Questions

View all questions & answers for the Professional Cloud Security Engineer exam

[Go to Exam](#)

### 📄 EXAM PROFESSIONAL CLOUD SECURITY ENGINEER TOPIC 1 QUESTION 49 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 49

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.

What should you do?

- A. Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
- B. Migrate the application into an isolated project using a "Lift & Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.
- C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.
- D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

[Show Suggested Answer](#)

by [rafaelc](#) at March 14, 2020, 10 a.m.

### Comments

Type your comment...



Submit

  **rafaelc** Highly Voted  4 years, 10 months ago

A or B. Leaning towards A

You have a deadline you cannot develop a new app so you have to lift and shift.

   upvoted 20 times

  **xhova** 4 years, 9 months ago

Answer is A.. You need VPC Flow Logs not "Firewall logs" stated in B

   upvoted 13 times

  **Table2022** 2 years, 3 months ago



xhova, you got it right!

   upvoted 3 times

  **smart123** 4 years, 6 months ago

I agree.

   upvoted 2 times

  **mynk29** 2 years, 11 months ago

Agree "Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly." if you disable all the VPC traffic there will be nothing to look into firewall logs.

   upvoted 8 times

  **YourFriendlyNeighborhoodSpider** Most Recent  4 months, 2 weeks ago

**Selected Answer: B**

The best option to complete the migration of the legacy application without putting your environment at risk is:

B. Migrate the application into an isolated project using a "Lift & Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.

Explanation:

Disable All Traffic: By disabling all traffic initially, you can ensure that no unauthorized traffic can access the application. This setup provides a secure environment.

Using Firewall Logs: This approach allows you to monitor what traffic is necessary for the application to function correctly after migration. You can analyze the Firewall logs to identify which ports and protocols are being used by the application, enabling you to refine your security configurations based on actual usage.

   upvoted 1 times

  **cskhachane** 11 months, 1 week ago

Option C:

   upvoted 1 times

  **okhascorpio** 11 months, 2 weeks ago

**Selected Answer: A**




B is not correct because Disabling all traffic within the VPC is too restrictive and hinders even initial testing. Analyzing firewall logs without any initial connectivity wouldn't be feasible.

   upvoted 2 times

  **Xoxoo** 1 year, 4 months ago

**Selected Answer: A**

Option B, C, and D involve making significant architectural changes (refactoring into microservices or using Cloud Functions) and disabling traffic, which might introduce complexities and risks. These options are more suitable when you have a better understanding of the application's requirements and can make informed decisions about its architecture and network policies. In your current scenario, option A provides a safe starting point for the migration process while you gather more information about the application's behavior.

   upvoted 3 times

  **ArizonaClassics** 1 year, 4 months ago

B. This option is similar to the first one but is more secure initially. The application is also migrated using a "Lift & Shift" approach. However, instead of enabling all internal TCP traffic, all traffic within the VPC is disabled. The Firewall logs (not exactly the most ideal tool but can give insights) are then used to determine what traffic is needed. This is more secure as it takes a deny-all-first approach.

   upvoted 1 times

  **amanshin** 1 year, 7 months ago

Option A is a valid approach, but it is not as secure as Option C. In Option A, the application is still exposed to the network.

Option A is a valid approach, but it is not as secure as Option C. In Option A, the application is still exposed to the network, even if it is in an isolated project. This means that if someone were to find a vulnerability in the application, they could potentially exploit it to gain access to the application.

In Option C, the application is isolated from the network by being deployed to a GKE cluster. This means that even if someone were to find a vulnerability in the application, they would not be able to exploit it to gain access to the application.

Additionally, Option C is more scalable and resilient than Option A. This is because a GKE cluster can be scaled up or down as needed, and it is more resistant to failure than a single VM.



Therefore, Option C is the more secure and scalable approach. However, if you are short on time, Option A may be a better option.

   upvoted 2 times

  **Joanale** 1 year, 8 months ago

A is a best option, remember you have the hurriest of the contract. Making microservices taking too long and have to know the detailed application architecture. Answer A.


   upvoted 2 times

  **Ric350** 1 year, 10 months ago

The answer is A. In real life you would NOT lift and shift an application especially not knowing the ports it uses nor any documentation. That'd be disruptive and cause an outage until you figured it out. You'd be out of a job! The question also clearly states "You want to complete the migration without putting your environment at risk!"

You'd have to refactor the application in parallel and makes sense if it's a legacy application. You'd want to modernize it with microservices so it can take advantage of all cloud features. If you simply lift and shift, the legacy app cannot take advantage of cloud services so what's the point? You still have the same problems except now you've moved it from on-prem to the cloud.

   upvoted 3 times

  **Ric350** 1 year, 10 months ago

Excuse me, C is the correct answer for the reasons listed below. You try lifting and shift a company application without the proper dependencies of how it works, cause a disruption or outage until you figure it out and let me know how that works for you and if you'll still have a job.

   upvoted 1 times

  **sameer2803** 1 year, 11 months ago

Answer is B.

even if you disable all traffic within VPC, the request to the application will hit the firewall and will get a deny ingress response. that way we get to know what port is It coming in. the same can be determined with allowing all traffic in (which exposes your application to the world ) but the question ends with "without putting your environment at risk"

   upvoted 2 times

  **pedrojorge** 2 years ago

**Selected Answer: B**

B, as A temporarily opens vulnerable paths in the system.

   upvoted 3 times

  **somnathmaddi** 2 years, 1 month ago

**Selected Answer: A**

Answer is A.. You need VPC Flow Logs not "Firewall logs" stated in B

   upvoted 4 times

  **Mixer5** 2 years, 2 months ago

**Selected Answer: A**

A since B disrupts the system. C and D are out of question if it's supposed to "just work".

   upvoted 4 times

  **Meyucho** 2 years, 2 months ago

**Selected Answer: B**

The difference between A and B is that, in the first, you allow all traffic so the app will work after migration and you can investigate which ports should be open and then take actions. If you go with B you will have a disruption window until figure out all ports needed but will not have any port unneeded port. So... if you asked to avoid disruption go with A and (as in this question) you are asked about security, go with B

   upvoted 4 times

  **pedrojorge** 2 years ago

The question never asks to avoid disruption, it asks to avoid risk, so the answer must be B.

   upvoted 2 times

  **AwesomeGCP** 2 years, 3 months ago

**Selected Answer: A**

A. Migrate the application into an isolated project using a "Lift & Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

👍 ↩ 🚩 upvoted 4 times

🗨️ 👤 **GPK** 3 years, 1 month ago

These questions are no more relevant as google has changed exam and made it really challenging now.

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **vicky.cyber** 3 years, 1 month ago

Could you please help us with recent dumps or guide which dump to be referred

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **Bwitch** 3 years ago

This one is accurate.

👍 ↩ 🚩 upvoted 2 times

🗨️ 👤 **rr4444** 3 years, 1 month ago

**Selected Answer: B**

B - VPC Flow Logs

Firewall logging only covers TCP and UDP, you explicitly don't know what the app does. That limitation is also important to the fact that implied deny all ingress and deny all egress rules are not covered by Firewall Logging. Plus you have to enable Firewall Logging per rule, so you'd have to have a rule for everything in advance - chicken and egg.... you don't know what is going on, so how could you!?

👍 ↩ 🚩 upvoted 1 times

🗨️ 👤 **rr4444** 3 years, 1 month ago

VPC FLOW logs is A!

I meant A!

👍 ↩ 🚩 upvoted 2 times

[Load full discussion...](#)



## Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)

