← 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 143 DISCUSSION**

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 143
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization hosts a financial services application running on Compute Engine instances for a third-party company. The third-party company's servers that will consume the application also run on Compute Engine in a separate Google Cloud organization. You need to configure a secure network connection between the Compute Engine instances. You have the following requirements:

☞ The network connection must be encrypted.
☞ The communication between servers must be over private IP addresses.
What should you do?

A. Configure a Cloud VPN connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.

B. Configure a VPC peering connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.

C. Configure a VPC Service Controls perimeter around your Compute Engine instances, and provide access to the third party via an access level.

D. Configure an Apigee proxy that exposes your Compute Engine-hosted application as an API, and is encrypted with TLS which allows access only to the third party.

Show Suggested Answer

by [deleted] at *Sept. 6, 2022, 5:46 a.m.*

Comments

Type your comment...

Submit

It's poorly worded and you will use service accont any communications and calls.
You can usd VPN, but you need a cloud router on both side, policy routing, etc. for the CEs to talk.
Thoughts?

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **desertlotus1211** 1 year, 10 months ago

I meant to say NO sense....

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **Kouuupobol** 2 years, 2 months ago

Selected Answer: A

Answer is A, because it is explicitly said that trafic must be encrypted.
Moreover, communication within the VPN use private IPs.

👍 ↩ 🚩 upvoted 3 times

☐ 👤 **deony** 2 years, 2 months ago

i don't think that Cloud VPN use public IP, but encrypted.
ref: https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview
> Traffic traveling between the two networks is encrypted by one VPN gateway and then decrypted by the other VPN gateway. This action protects your data as it travels over the internet.

but, with cloud interconnect, Cloud VPN can use private IP.
i think it's too heavy works using VPN with cloud interconnect instead of using VPC peering.

👍 ↩ 🚩 upvoted 2 times

☐ 👤 **deony** 2 years, 2 months ago

typo: i don't think -> i think

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **TNT87** 2 years, 3 months ago

Selected Answer: B

Answer B

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **alleinallein** 2 years, 3 months ago

Why not A? Any arguments?

👍 ↩ 🚩 upvoted 2 times

☐ 👤 **TonytheTiger** 2 years, 8 months ago

B:
https://cloud.google.com/vpc/docs/vpc-peering

👍 ↩ 🚩 upvoted 3 times

☐ 👤 **TonytheTiger** 2 years, 8 months ago

Sorry - Ans C - Key point "separate Google Cloud Organization"
Private Service Connect allows private consumption of services across VPC networks that belong to different groups, teams, projects, or organizations.
https://cloud.google.com/vpc/docs/private-service-connect

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **fad3r** 2 years, 4 months ago

You are right and wrong, You are right that yes Private Service Connect does indeed do this. You are wrong because that is not what C says. It says VPC Service Controls which is definitely wrong.

👍 ↩ 🚩 upvoted 1 times

☐ 👤 **Littleivy** 2 years, 8 months ago

Selected Answer: B

B

VPC Network Peering gives you several advantages over using external IP addresses or VPNs to connect networks

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

👍 ↩ 🚩 upvoted 3 times

☐ 👤 **AzureDP900** 2 years, 8 months ago

B. Configure a VPC peering connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.

👍 ↩ 🚩 upvoted 2 times

soltium 2 years, 9 months ago

A and B is correct, Cloud VPN are encrypted, VPC Peering might be unencrypted but this docs said it's encrypted. https://cloud.google.com/docs/security/encryption-in-transit#virtual_machine_to_virtual_machine

👍 ↩ 🏳 upvoted 3 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: B

B. Configure a VPC peering connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.

👍 ↩ 🏳 upvoted 2 times

zellck 2 years, 10 months ago

Selected Answer: B

B is the answer.

👍 ↩ 🏳 upvoted 2 times

[Removed] 2 years, 10 months ago

Selected Answer: B

final B

👍 ↩ 🏳 upvoted 2 times

GHOST1985 2 years, 10 months ago

Selected Answer: B

Google encrypts and authenticates data in transit at one or more network layers when data moves outside physical boundaries not controlled by Google or on behalf of Google. All VM-to-VM traffic within a VPC network and peered VPC networks is encrypted. https://cloud.google.com/docs/security/encryption-in-transit#cio-level_summary

👍 ↩ 🏳 upvoted 4 times

Load full discussion...