← 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 134 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 134

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You need to set up a Cloud interconnect connection between your company's on-premises data center and VPC host network. You want to make sure that on-premises applications can only access Google APIs over the Cloud Interconnect and not through the public internet. You are required to only use APIs that are supported by VPC Service Controls to mitigate against exfiltration risk to non-supported APIs. How should you configure the network?

A. Enable Private Google Access on the regional subnets and global dynamic routing mode.

B. Set up a Private Service Connect endpoint IP address with the API bundle of "all-apis", which is advertised as a route over the Cloud interconnect connection.

C. Use private.googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the connection.

D. Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection.

Show Suggested Answer

by 👤 **Nicky1402** at *May 9, 2022, 9:49 a.m.*

Comments

Type your comment...

Nicky1402 **Highly Voted** 👍 2 years, 8 months ago

I think the correct answer is D.
It is mentioned in the question: "You are required to only use APIs that are supported by VPC Service Controls", from which we can understand that we cannot use private.googleapis.com. Hence, option A & C can be eliminated.
API bundle with all-apis is mentioned in option B which is wrong as we want to use only those APIs supported by VPC service controls. Hence, option B can be eliminated.
Option D has all the solutions we need.

https://cloud.google.com/vpc/docs/private-service-connect

An API bundle:
All APIs (all-apis): most Google APIs
(same as private.googleapis.com).
VPC-SC (vpc-sc): APIs that VPC Service Controls supports
(same as restricted.googleapis.com).
VMs in the same VPC network as the endpoint (all regions)
On-premises systems that are connected to the VPC network that contains the endpoint

👍 ↩ 🚩 upvoted 13 times

    AzureDP900 2 years, 2 months ago

    Yes, It is D

    👍 ↩ 🚩 upvoted 1 times

        AzureDP900 2 years, 2 months ago

        D. Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection.

        👍 ↩ 🚩 upvoted 1 times

dija123 **Most Recent** ⊘ 10 months, 1 week ago

Selected Answer: D

Answer is D

👍 ↩ 🚩 upvoted 1 times

shayke 2 years, 1 month ago

Selected Answer: D

D- route from on prem

👍 ↩ 🚩 upvoted 1 times

samuelmorher 2 years, 1 month ago

Selected Answer: D

it's D

👍 ↩ 🚩 upvoted 2 times

marmar11111 2 years, 2 months ago

Selected Answer: D

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

Choose restricted.googleapis.com when you only need access to Google APIs and services that are supported by VPC Service Controls.

👍 ↩ 🚩 upvoted 1 times

AwesomeGCP 2 years, 3 months ago

Selected Answer: D

D. Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection.

👍 ↩ 🚩 upvoted 2 times

zellck 2 years, 4 months ago

Selected Answer: D

D is the answer.

https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid#config-choose-domain
If you need to restrict users to just the Google APIs and services that support VPC Service Controls, use restricted.googleapis.com. Although VPC Service Controls are enforced for compatible and configured services, regardless of the domain you use, restricted.googleapis.com provides additional risk mitigation for data exfiltration. Using restricted.googleapis.com denies access to Google APIs and services that are not supported by VPC Service Controls.

👍 ↩ 🚩 upvoted 1 times

⊟ 👤 **bnikunj** 2 years, 4 months ago

D is answer, https://cloud.google.com/vpc/docs/configure-private-service-connect-apis#supported-apis

The all-apis bundle provides access to the same APIs as private.googleapis.com

Choose vpc-sc when you only need access to Google APIs and services that are supported by VPC Service Controls. The vpc-sc bundle does not permit access to Google APIs and services that do not support VPC Service Controls. 1

👍 ↩ 🚩 upvoted 1 times

⊟ 👤 **cloudprincipal** 2 years, 7 months ago

Selected Answer: D

Will agree with the others

👍 ↩ 🚩 upvoted 2 times

⊟ 👤 **cloudprincipal** 2 years, 7 months ago

This is actually specified in the documentation: https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid#config-choose-domain

👍 ↩ 🚩 upvoted 3 times

⊟ 👤 **ExamQnA** 2 years, 8 months ago

Ans: D

Note: If you need to restrict users to just the Google APIs and services that support VPC Service Controls, use restricted.googleapis.com.

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

👍 ↩ 🚩 upvoted 3 times