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 54 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 54

Topic #: 1

[All Professional Cloud Security Engineer Questions]

Your team needs to make sure that their backend database can only be accessed by the frontend application and no other instances on the network.

How should your team design this network?

A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.

B. Create a different subnet for the frontend application and database to ensure network isolation.

C. Create two VPC networks, and connect the two networks using Cloud VPN gateways to ensure network isolation.

D. Create two VPC networks, and connect the two networks using VPC peering to ensure network isolation.

Show Suggested Answer

by mlyu at *Sept. 1, 2020, 8:39 a.m.*

Comments

Type your comment...

Submit

singhjoga Highly Voted 4 years ago

Although A is correct, but B would be more secure when combined with firewall rules to restrict traffic based on subnets.
Ideal solution would be to use Service Account based firewall rules instead of tag based. See the below paragragraph from

ideal solution would be to use Service Account based firewall rules instead of tag based. See the below paragragraph from https://cloud.google.com/solutions/best-practices-vpc-design

"However, even though it is possible to uses tags for target filtering in this manner, we recommend that you use service accounts where possible. Target tags are not access-controlled and can be changed by someone with the instanceAdmin role while VMs are in service. Service accounts are access-controlled, meaning that a specific user must be explicitly authorized to use a service account. There can only be one service account per instance, whereas there can be multiple tags. Also, service accounts assigned to a VM can only be changed when the VM is stopped"

upvoted 7 times

ThisisJohn 3 years, 1 month ago

You may be right but B doesn't mention anything about firewall rules, thus we need to assume there will be communication between both subnets

upvoted 2 times

Aiffone 2 years, 7 months ago

I'm inclined to go with A too because without firewall rules the subnets in B would ensure there is no communication at all due to default implicit rules.

upvoted 1 times

CHECK666 Highly Voted 4 years, 4 months ago

A is the answer, use network tags.

upvoted 6 times

[Removed] Most Recent 1 year, 6 months ago

Selected Answer: A

"A"
The choice is between A and B. Even though subnet isolation is recommended (which would make B correct), subnet isolation alone without accompanying firewall rules does not ensure security.
Only A emphasizes the use of firewall which makes it more correct than B.

Reference:
https://cloud.google.com/architecture/best-practices-vpc-design#target_filtering

upvoted 3 times

Portugapt 10 months, 1 week ago

But here the question goes into the design of the network, not the specific implementation details. For design, B makes more sense.

upvoted 1 times

AzureDP900 2 years, 2 months ago

A is correct , rest of the answers doesn't make any sence

upvoted 1 times

azureaspirant 2 years, 2 months ago

@AzureDP900: Cleared AWS Solution Architect Professional (SAP - CO1) on the last date. followed your answers. Cleared 5 GCP Certificates. Glad that you are here.

upvoted 2 times

AwesomeGCP 2 years, 3 months ago

Selected Answer: A

A. Create an ingress firewall rule to allow access only from the application to the database using firewall tags.

upvoted 1 times

zqwiklabs 3 years, 10 months ago

A is definitely incorrect

upvoted 4 times

mistryminded 3 years, 1 month ago

This one is confusing but cannot be A because it says 'Firewall tags'. There is no such thing as firewall tags, only 'Network tags'.

upvoted 2 times

desertlotus1211 3 years, 10 months ago

Answer is D: you'd want the DB in a separate VPC. Allow vpc peering and connect the Front End's backend to the DB. Don't get confused by the question saying 'front end' Front end only means public facing...

upvoted 1 times

AzureDP900 2 years, 2 months ago

A is correct

upvoted 1 times

Jane111 3 years, 9 months ago

you need to read basic concepts again

upvoted 7 times

DebasishLowes 3 years, 11 months ago

Ans : A

upvoted 3 times

mlyu 4 years, 5 months ago

Agree with A

upvoted 2 times