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 163 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 163

Topic #: 1

[All Professional Cloud Security Engineer Questions]

You need to audit the network segmentation for your Google Cloud footprint. You currently operate Production and Non-Production infrastructure-as-a-service
(IaaS) environments. All your VM instances are deployed without any service account customization.
After observing the traffic in your custom network, you notice that all instances can communicate freely `" despite tag-based VPC firewall rules in place to segment traffic properly `" with a priority of 1000. What are the most likely reasons for this behavior?

A. All VM instances are missing the respective network tags.

B. All VM instances are residing in the same network subnet.

C. All VM instances are configured with the same network route.

D. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 999. E . A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 1001.

Show Suggested Answer

by redgoose6810 at *Oct. 3, 2022, 6:13 a.m.*

Comments

Type your comment...

Submit

nah99 8 months, 1 week ago

Please separate answers D & E so it's less confusing

upvoted 3 times

Mr_MIXER007 11 months ago

Selected Answer: AD

All VM instances are missing the respective network tags + A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 999

upvoted 1 times

Bettoxicity 1 year, 3 months ago

Selected Answer: A

A

This scenario would bypass the tag-based firewall rules you've implemented. If VMs lack the intended tags, the firewall rules wouldn't be able to identify and filter traffic based on those tags.

upvoted 1 times

dija123 1 year, 4 months ago

Selected Answer: AD

Answers A,D

upvoted 1 times

desertlotus1211 1 year, 10 months ago

Remember you can ONLY use EITHER service account or tags to filter traffic. You cannot mix.
https://medium.com/google-cloud/gcp-cloud-vpc-firewall-with-service-accounts-9902661a4021#:~:text=VPC%20firewall%20rules%20let%20you,on%20a%20per%2Dinstance%20basis.

Answers A,D

upvoted 3 times

gcpengineer 2 years, 2 months ago

Selected Answer: D

D is the only answer

upvoted 4 times

Ric350 2 years, 3 months ago

How is D even an option and considered? The question itself clearly states "All your VM instances are deployed WITHOUT any service account customization." That means the firewall rule would NOT let any traffic through as there's no SA on the vm's to apply the rule. A is a likely scenario and could easily be overlooked when deploying. B is very unlikely and one big flat network. C is also likely due to admin mistake and overlooking like A. I'd go with A and C as the answer here. Unless I'm interpreting it wrong or missing something here.

upvoted 3 times

> **Bettoxicity** 1 year, 3 months ago
>
> You are right, also, how is a rule with priority 1001 going to have priority over another rule with 1000?
>
> upvoted 1 times
>
> **gcpengineer** 2 years, 2 months ago
>
> it means all VMs r using same SA
>
> upvoted 5 times

GCParchitect2022 2 years, 6 months ago

Selected Answer: AD

A. All VM instances are missing the respective network tags.
D. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 999.

If all the VM instances in your Google Cloud environment are able to communicate freely despite tag-based VPC firewall rules in place, it is likely that the instances are missing the necessary network tags. Without the appropriate tags, the firewall rules will not be able to properly segment the traffic. Another possible reason for this behavior could be the existence of a VPC firewall rule that allows traffic between source and target instances based on the same service account, with a priority of 999. This rule would take precedence over the tag-based firewall rules with a priority of 1000. It is unlikely that all the VM instances are residing in the same network subnet or configured with the same network route, or that there is a VPC firewall rule allowing traffic with a priority of 1001.

upvoted 4 times

zanhsieh 2 years, 7 months ago

I hit this question on the real exam. It supposed to choose TWO answers. I would pick CD as my answer.
A. WRONG. The question already stated "despite tag-based VPC firewall rules in place to segment traffic properly ... with a

A: WRONG. The question already stated "despite tag-based VPC firewall rules in place to segment traffic properly -- with a priority of 1000" so network tags are already in-place.
B: WRONG. The customer could set default network across the globe, and then VMs inside one region subnet could ping VMs inside another region subnet.
C: CORRECT.
D: CORRECT.
E: WRONG. Firewall rules with higher priority shall have less than 1000 as the question stated.

upvoted 1 times

theereechee 2 years, 7 months ago

A & D are correct. You can have tag-based firewall rule in place, but without actually applying the tags to instances, the firewall rule is useless/meaningless.

upvoted 5 times

gcpengineer 2 years, 2 months ago

but only few tags r missing...so all vms shd not able to talk

upvoted 1 times

zanhsieh 2 years, 7 months ago

I hit this question. It supposed to select TWO answers. I would say Option D definitely would be the right answer. The rest one I no idea.

upvoted 2 times

adelynllllllllll 2 years, 8 months ago

D: a 999 will overwrite 1000

upvoted 1 times

Littleivy 2 years, 8 months ago

Selected Answer: D

The answer is D

upvoted 2 times

rotorclear 2 years, 9 months ago

Selected Answer: AD

1001 is lower priority

upvoted 2 times

soltium 2 years, 9 months ago

D. priority 999 is a higher priority than 1000, so if 999 has allow all policy then any deny policy with lower priority will not be applied.

upvoted 3 times

JoeBar 1 year, 10 months ago

really confusing, D is enough for traffic to be allowed prior hitting the tagbased rule, but if you combine A & E same applies, if A (missing Tag) then the 1000 rules is missed, but traffic is therefore allowed by 1001 so AE should also work while D is a standalone condition.
Really can't make a decision here

upvoted 1 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: C

C. All VM instances are configured with the same network route.

upvoted 2 times

dat987 2 years, 9 months ago

Do you have any documents for this? Thanks

upvoted 1 times

redgoose6810 2 years, 9 months ago

maybe A . any idea please.

upvoted 3 times

maxth3mad 2 years, 9 months ago

maybe B too ... same subnet ...

upvoted 3 times

maxth3mad 2 years, 9 months ago

but if a firewall rule is in place, probably A

upvoted 1 times

EXAMTOPICS

Platform

- Home
- Examtopics PRO
- All Exams
- Training Courses