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 65 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 65
Topic #: 1
[All Professional Cloud Security Engineer Questions]

A customer has an analytics workload running on Compute Engine that should have limited internet access.
Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet.
The Compute Engine instances now need to reach out to the public repository to get security updates.
What should your team do?

A. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority greater than 1000.

B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.

C. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority greater than 1000.

D. Create an egress firewall rule to allow traffic to the hostname of the repository with a priority less than 1000.

Show Suggested Answer

by mlyu at *Sept. 3, 2020, 2:44 a.m.*

Comments

Type your comment...

Submit

dtmtor Highly Voted 4 years, 4 months ago

Answer is B. Lower number is higher priority and dest is only IP ranges in firewall rules

upvoted 26 times

Rithac Highly Voted 4 years, 1 month ago

I think I am confusing myself by overthinking the wording of this question. I know the answer is A or B since "using hostname is not one of the options in firewall egress rule destination" I also know that "The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities." I know that I could resolve this by setting TCP port 80 rule to a priority of 500 (smaller number, but higher priority) and be done. Where i'm second guessing myself, is Google referring to the integer or strictly priority? If integer then i'd choose B "priority less than 1000 (smaller number)", if priority then i'd choose A "priority greater than 1000" (still the lower number). Have I thoroughly confused this question? I"m leaning toward the answer being "A:

upvoted 5 times

BPzen Most Recent 8 months ago

Selected Answer: B

While the priority is correct, Google Cloud firewall rules do not support hostname-based filtering. You must use a CIDR range.

upvoted 1 times

madcloud32 1 year, 4 months ago

Selected Answer: B

B is correct.

upvoted 1 times

shayke 2 years, 7 months ago

Selected Answer: B

Ans in B lower number higher priority

upvoted 3 times

Littleivy 2 years, 8 months ago

Selected Answer: B

Answer is B

upvoted 3 times

GHOST1985 2 years, 8 months ago

Selected Answer: B

https://cloud.google.com/vpc/docs/firewalls#priority_order_for_firewall_rules

upvoted 4 times

AzureDP900 2 years, 8 months ago

B is correct

upvoted 2 times

Premumar 2 years, 9 months ago

Selected Answer: B

First filter is priority should be less than 1000. So, option A and C are rejected. Then, we use CIDR range to allow firewall. So, the final answer is B.

upvoted 3 times

AwesomeGCP 2 years, 9 months ago

Selected Answer: B

B. Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.
Firewall rules only support IPv4 connections. When specifying a source for an ingress rule or a destination for an egress rule by address, you can only use an IPv4 address or IPv4 block in CIDR notation. So Answer is B

upvoted 4 times

piyush_1982 3 years ago

Selected Answer: A

The correct answer is A.
As per the link https://cloud.google.com/vpc/docs/firewalls#rule_assignment

Lowest priority in the firewall rule is 65535. So in order for a rule to be of higher priority than 1000 the rule should have a priority of number less than 1000.

upvoted 2 times

Premumar 2 years, 9 months ago

Your explanation is correct. But, option you selected is wrong. It has to be option B.

upvoted 3 times

DebasishLowes 4 years, 4 months ago

Ans : B

upvoted 3 times

ronron89 4 years, 7 months ago

Answer: B
https://cloud.google.com/vpc/docs/firewalls#rule_assignment
The priority of the second rule determines whether TCP traffic to port 80 is allowed for the webserver targets:

If the priority of the second rule is set to a number greater than 1000, it has a lower priority, so the first rule denying all traffic applies.

If the priority of the second rule is set to 1000, the two rules have identical priorities, so the first rule denying all traffic applies.

If the priority of the second rule is set to a number less than 1000, it has a higher priority, thus allowing traffic on TCP 80 for the webserver targets. Absent other rules, the first rule would still deny other types of traffic to the webserver targets, and it would also deny all traffic, including TCP 80, to instances without the webserver tag.

upvoted 4 times

Raushanr 4 years, 10 months ago

The firewall rule priority is an integer from 0 to 65535, inclusive. Lower integers indicate higher priorities. If you do not specify a priority when creating a rule, it is assigned a priority of 1000.

upvoted 1 times

Raushanr 4 years, 10 months ago

Answer-B

upvoted 4 times

ownez 4 years, 10 months ago

It should be B.

Firewall rules can be only specify by IPv4 address or IPv4 block in CIDR.
And it must be lesser priority than 1000 because if more than that, it will overwrite the deny rule.

upvoted 2 times

ownez 4 years, 10 months ago

Sorry It should be A.

"Priority: the numeric evaluation order of the rule. A rule with a priority of 1 is evaluated first. Priorities must be unique for each rule. A good practice is to give rules priority numbers that allow later insertion (such as 100, 200, 300)."

upvoted 1 times

ownez 4 years, 10 months ago

Correction. B

upvoted 3 times

mlyu 4 years, 10 months ago

Ans should be A
using hostname is not one of the options in firewall egress rule destination
https://cloud.google.com/vpc/docs/firewalls#gcp_firewall_rule_summary_table

upvoted 2 times

EXAMTOPICS

Platform

- Home
- All Exams
- Examtopics PRO
- Training Courses

© 2024 ExamTopics