Google Discussions

EXAM ASSOCIATE CLOUD ENGINEER TOPIC 1 QUESTION 151 DISCUSSION

Actual exam question from Google's Associate Cloud Engineer
Question #: 151
Topic #: 1
[All Associate Cloud Engineer Questions]

You are working with a user to set up an application in a new VPC behind a firewall. The user is concerned about data egress. You want to configure the fewest open egress ports. What should you do?

A. Set up a low-priority (65534) rule that blocks all egress and a high-priority rule (1000) that allows only the appropriate ports.

B. Set up a high-priority (1000) rule that pairs both ingress and egress ports.

C. Set up a high-priority (1000) rule that blocks all egress and a low-priority (65534) rule that allows only the appropriate ports.

D. Set up a high-priority (1000) rule to allow the appropriate ports.

Show Suggested Answer

by MohammedGhouse at *Aug. 12, 2020, 10:35 a.m.*

Comments

ESP_SAP Highly Voted 4 years, 2 months ago

Correct Answer is (A):

Implied rules
Every VPC network has two implied firewall rules. These rules exist, but are not shown in the Cloud Console:

Implied allow egress rule. An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination, except for traffic blocked by Google Cloud. A higher priority firewall rule may restrict outbound access. Internet access is allowed if no other firewall rules deny outbound traffic and if the instance has an external IP address or uses a Cloud NAT instance. For more information, see Internet access requirements.

Implied deny ingress rule. An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them. A higher priority rule might allow incoming access. The default network includes some additional rules that override this one, allowing certain types of incoming connections.

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

upvoted 43 times

patashish 2 years, 3 months ago

The correct answer is C

upvoted 1 times

ryumada 2 years, 2 months ago

You should visit the documentation link he attached. He's copy those statements from the Google Docs.

upvoted 2 times

Roro_Brother 2 years, 3 months ago

Listen that guy because he is right

upvoted 1 times

bobthebuilder55110 Highly Voted 2 years, 2 months ago

Selected Answer: A

Answer is (A) :
First I was going with C but then I read the question again, let's try to understand both options here, the goal is to deny egress and only allow some ports for some functions to perform. If we go with C, lower the number higher the priority (1000) so the rule with this priority 1000 will overwrite (65534), so If we allow only appropriate ports it will be overwritten with the high-priority (1000) rule and all the egress traffic will be blocked.
Remember the goal here is to block egress but not all of it since we still want to configure the fewest open ports and this is statefull meaning for open ports traffic will be both ways.
A fits this condition where it is saying we block all traffic but the required ports are kept open with higher priority which will only allow the required traffic to leave the network.

upvoted 16 times

Cynthia2023 Most Recent 9 months, 3 weeks ago

Selected Answer: A

Default Egress Behavior: In Google Cloud VPCs, the default behavior is to allow all egress traffic. To restrict egress traffic effectively, you need to explicitly set up firewall rules.

Blocking All Egress Traffic: The low-priority rule (priority 65534, near the lowest priority) should be configured to block all egress traffic. This creates a baseline rule that denies all egress traffic by default.

Allowing Specific Ports: The high-priority rule (priority 1000, indicating a higher priority) should be set to allow egress traffic only on the specific ports that are required for the application. Since firewall rules are evaluated in order of priority, this rule will override the default block for these specific ports.

upvoted 2 times

jimmydice 11 months, 3 weeks ago

Correct answer is C: By implementing a high-priority rule to block all egress traffic (since it has a lower number than lower-priority rules), and a low-priority rule to selectively allow specific necessary egress ports (with a higher number), you minimize open egress ports to only the required ones while restricting the rest.

upvoted 2 times

scanner2 1 year, 1 month ago

Selected Answer: A

The rule is evaluated on higher priority to lower priority and depends first come first serve basis.
https://cloud.google.com/firewall/docs/firewall-policies-overview#rule-evaluation

upvoted 1 times

Captain1212 1 year, 1 month ago

Selected Answer: A

A is the correct answer

upvoted 2 times

fragment137 1 year, 10 months ago

Selected Answer: A

Correct answer is A.

Answer will not be D, because Egress traffic is Allowed by default. You will have to explicitly set the rule blocking outbound traffic.

upvoted 1 times

ryumada 2 years, 2 months ago

Selected Answer: A

Read ESP_SAP comment for the explanation. He explains it clearly.

upvoted 1 times

sonuricky 2 years, 2 months ago

C is the correct answer

upvoted 1 times

gscharly 2 years, 2 months ago

Selected Answer: A

A: is the answer

upvoted 1 times

Roro_Brother 2 years, 3 months ago

Selected Answer: A

Correct answer is A

upvoted 1 times

patashish 2 years, 3 months ago

Correct Answer is C

upvoted 1 times

patashish 2 years, 3 months ago

Hint : All rules are stateful.
VPC firewall rules are stateful. When a connection is allowed through the firewall in either direction, return traffic matching this connection is also allowed. You cannot configure a firewall rule to deny associated response traffic.

As per question , we want to restrict egress traffic.
So focus to restrict egress traffic based on priority of rules.
Allow incoming traffic for appropriate traffic and block all traffic and allow only which are required.

Hence , as per my view C should be correct answer

upvoted 3 times

mani098 2 years, 4 months ago

Selected Answer: D

A incorrect 65534 that blocks all ingress, not egress (except few default ports)
D is correct.

upvoted 3 times

patashish 2 years, 3 months ago

But why D is correct ? Why not C ?

D is more generic , As per question , need to focus on egress traffic

upvoted 1 times

pnVino27 2 years, 10 months ago

Selected Answer: A

Correct Answer is A

upvoted 3 times

maggieli 2 years, 11 months ago

I vote A is correct. Block all port in gress and set low-priority.

upvoted 2 times

aamirahal 3 years ago

A is correct

upvoted 2 times

vvkds 3 years, 2 months ago

Correct answer is A. Firewall rules are executed based on the priority.

upvoted 2 times

Load full discussion...