

[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 239 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 239

Topic #: 1

[\[All Professional Cloud Security Engineer Questions\]](#)

You control network traffic for a folder in your Google Cloud environment. Your folder includes multiple projects and Virtual Private Cloud (VPC) networks. You want to enforce on the folder level that egress connections are limited only to IP range 10.58.5.0/24 and only from the VPC network "dev-vpc". You want to minimize implementation and maintenance effort.

What should you do?



- A. 1. Leave the network configuration of the VMs in scope unchanged.
2. Create a new project including a new VPC network "new-vpc".
3. Deploy a network appliance in "new-vpc" to filter access requests and only allow egress connections from "dev-vpc" to 10.58.5.0/24.
- B. 1. Leave the network configuration of the VMs in scope unchanged.
2. Enable Cloud NAT for "dev-vpc" and restrict the target range in Cloud NAT to 10.58.5.0/24.
- C. 1. Attach external IP addresses to the VMs in scope.
2. Define and apply a hierarchical firewall policy on folder level to deny all egress connections and to allow egress to IP range 10.58.5.0/24 from network dev-vpc.
- D. 1. Attach external IP addresses to the VMs in scope.
2. Configure a VPC Firewall rule in "dev-vpc" that allows egress connectivity to IP range 10.58.5.0/24 for all source addresses in this network.

[Show Suggested Answer](#)

Comments

Type your comment...

[Submit](#)

  **BPzen** 8 months ago

Selected Answer: C

Hierarchical Firewall Policy:

These policies are defined at the organization or folder level and are inherited by all projects under the folder. You can use this to enforce a rule that allows egress traffic only to the specific IP range (10.58.5.0/24) from the dev-vpc network while blocking all other egress traffic.

This minimizes ongoing maintenance because the policy applies automatically to all resources in the folder.

External IP Addresses:

By attaching external IP addresses to the VMs, you ensure they can communicate outside the VPC, subject to the egress policies defined at the folder level.

   upvoted 2 times

  **MoAk** 8 months ago

Selected Answer: C

hmm this is a tricky one. between B and C i am leaning more towards C but only because of the wording in the Q itself, specifically 'enforce on the folder level'.

For me all options are pants but I feel the Q is intending to test the knowledge about hierarchical firewall policies. Further, cloud NAT itself would not be a selected product to 'enforce' controls intended by the use case in this Q.



   upvoted 1 times

  **Mr_MIXER007** 10 months, 3 weeks ago

Selected Answer: C

Cloud NAT is primarily for providing internet access to instances in private subnets. It doesn't offer the granular control needed to restrict egress traffic based on source VPC networks

   upvoted 1 times

  **3d9563b** 1 year ago

Selected Answer: C

Applying a hierarchical firewall policy at the folder level ensures centralized control of egress traffic across all networks and projects within the folder, minimizing implementation and maintenance efforts while enforcing the required network traffic constraints.

   upvoted 1 times

  **pico** 1 year, 2 months ago

Selected Answer: B

But I'm not agree 100% with any of them. B & C are the less worst but not the good ones.

C is not complain with: on the folder level

B is not complain with: minimize implementation and maintenance effort because of the add external ip addresses to the VMs step

   upvoted 1 times

  **Betotoxicity** 1 year, 3 months ago

Selected Answer: C

-Folder-Level Policy: A hierarchical firewall policy applied at the folder level ensures consistent enforcement across all VPC networks within that folder. This simplifies management compared to individual project or VPC configurations.

-Deny All Egress with Allow Rule: Setting a "deny all egress" rule as the default policy at the folder level strengthens security by explicitly blocking outbound traffic. A separate rule specifically allows egress to the desired IP range (10.58.5.0/24) from the "dev-vpc" network, meeting your requirements.

-No VM Configuration Changes: This approach avoids modifying individual VM network configurations, reducing complexity and potential errors.

   upvoted 1 times

  **dija123** 1 year, 4 months ago

Selected Answer: B

allowing egress to the entire 10.58.5.0/24 network does not make any sense, enabling Cloud NAT for "dev-vpc" with the target range restricted to 10.58.5.0/24 provides a straightforward and efficient way to enforce egress connections on the folder level, meeting your criteria of minimal implementation and maintenance effort.

👍 ↩ 🚩 upvoted 2 times

🗄️ 👤 **adb4007** 1 year, 5 months ago

Selected Answer: C

In my opinion the less worth option is C.

A is wrong because use an other VPC in other Network cannot help to filter egress access

B is wrong for me because NAT doesn't allow us to limit access even NAT is could be make between VPC.

D by default all egress connections are allow add a rule make no change for me.

in C you make a rule applie on all folder that deny egress by default and allow the source network as expected. I don't understand the fact of add a public ip adress that don't help for me but it is not blocking.

👍 ↩ 🚩 upvoted 1 times

🗄️ 👤 **b6f53d8** 1 year, 5 months ago

Selected Answer: B

Why not B ?

👍 ↩ 🚩 upvoted 3 times

🗄️ 👤 **b6f53d8** 1 year, 5 months ago

But mentioned IP range is internal, so why we need External IP ? In my opinion all answers are bad

👍 ↩ 🚩 upvoted 3 times

🗄️ 👤 **winston9** 1 year, 5 months ago

NAT can be used to route internal traffic to other VPCs also.

Cloud NAT lets certain resources in Google Cloud create outbound connections to the internet or to other Virtual Private Cloud (VPC) networks.

<https://cloud.google.com/nat/docs/overview>

👍 ↩ 🚩 upvoted 2 times

🗄️ 👤 **NaikMN** 1 year, 7 months ago

Selected Answer: C

<https://cloud.google.com/firewall/docs/firewall-policies-examples>

👍 ↩ 🚩 upvoted 1 times

🗄️ 👤 **MisterHairy** 1 year, 8 months ago

Selected Answer: C

The correct answer is C. 1. Attach external IP addresses to the VMs in scope. 2. Define and apply a hierarchical firewall policy on folder level to deny all egress connections and to allow egress to IP range 10.58.5.0/24 from network dev-vpc.

This approach allows you to control network traffic at the folder level. By attaching external IP addresses to the VMs in scope, you can ensure that the VMs have a unique, routable IP address for outbound connections. Then, by defining and applying a hierarchical firewall policy at the folder level, you can enforce that egress connections are limited to the specified IP range and only from the specified VPC network.

👍 ↩ 🚩 upvoted 1 times



Platform

> Home

> Examtopics PRO

> All Exams

> Training Courses

