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 261 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer
Question #: 261
Topic #: 1
[All Professional Cloud Security Engineer Questions]

Your organization utilizes Cloud Run services within multiple projects underneath the non-production folder which requires primarily internal communication. Some services need external access to approved fully qualified domain names (FQDN) while other external traffic must be blocked. Internal applications must not be exposed. You must achieve this granular control with allowlists overriding broader restrictions only for designated VPCs. What should you do?

A. Implement a global-level allowlist rule for the necessary FQDNs within a hierarchical firewall policy. Apply this policy across all VPCs in the organization and configure Cloud NAT without any additional filtering.

B. Create a folder-level deny-all rule for outbound traffic within a hierarchical firewall policy. Define FQDN allowlist rules in separate policies and associate them with the necessary VPCs. Configure Cloud NAT for these VPCs.

C. Create a project-level deny-all rule within a hierarchical structure and apply it broadly. Override this rule with separate FQDN allowlists defined in VPC-level firewall policies associated with the relevant VPCs.

D. Configure Cloud NAT with IP-based filtering to permit outbound traffic only to the allowlist d FQDNs' IP ranges. Apply Cloud NAT uniformly to all VPCs within the organization's folder structure.

Show Suggested Answer

by yokoyan at *Sept. 6, 2024, 1:29 a.m.*

Comments

Type your comment...

Submit

KLei 7 months, 1 week ago

Selected Answer: B

Cloud Public NAT support not only the VM instances but also Cloud Run
https://cloud.google.com/nat/docs/overview#supported-resources

upvoted 1 times

Pime13 7 months, 3 weeks ago

Selected Answer: B

This approach allows you to:

Enforce a deny-all rule at the folder level, ensuring that no outbound traffic is allowed by default.
Create specific allowlist rules for the approved FQDNs and apply these rules to the necessary VPCs, providing the required external access.
Configure Cloud NAT to handle the outbound traffic for these VPCs, ensuring that the traffic is routed correctly while adhering to the allowlist rules.

upvoted 1 times

MoAk 8 months, 1 week ago

Selected Answer: B

Only answer that makes sense to me.

upvoted 1 times

yokoyan 10 months, 3 weeks ago

Selected Answer: B

I think it's B.

upvoted 1 times