

 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 292 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 292

Topic #: 1

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

You are implementing a new web application on Google Cloud that will be accessed from your on-premises network. To provide protection from threats like malware, you must implement transport layer security (TLS) interception for incoming traffic to your application. What should you do?

- A. Configure Secure Web Proxy. Offload the TLS traffic in the load balancer, inspect the traffic, and forward the traffic to the web application.
- B. Configure an internal proxy load balancer. Offload the TLS traffic in the load balancer inspect, the traffic and forward the traffic to the web application.
- C. Configure a hierarchical firewall policy. Enable TLS interception by using Cloud Next Generation Firewall (NGFW) Enterprise.
- D. Configure a VPC firewall rule. Enable TLS interception by using Cloud Next Generation Firewall (NGFW) Enterprise.

[Show Suggested Answer](#)

by  yokoyan at Sept. 6, 2024, 1:54 a.m.

Comments

Type your comment...

[Submit](#)

🗄️  **snti9999** 3 months, 1 week ago

Selected Answer: C

You need NGFW.

👍 ↩️ 🚩 upvoted 1 times

🗄️  **YourFriendlyNeighborhoodSpider** 4 months, 1 week ago

Selected Answer: C

Google Cloud's Cloud Next Generation Firewall (NGFW) Enterprise includes TLS inspection capabilities, which allow you to decrypt and inspect encrypted traffic for threats before it reaches your web application. This is essential for protecting against malware and other threats embedded in encrypted traffic.

A hierarchical firewall policy allows you to enforce firewall rules at the organization or folder level, ensuring consistent security policies across multiple projects.
Why Not the Other Options?

A. Secure Web Proxy + Load Balancer

Google Cloud does not offer a native Secure Web Proxy with TLS interception for incoming traffic. Load balancers in Google Cloud do not provide deep TLS interception for security inspection.

👍 ↩️ 🚩 upvoted 1 times

🗄️  **Popa** 5 months ago

Selected Answer: A

Here's why:

Secure Web Proxy is specifically designed to provide advanced security measures, including TLS interception. It allows you to offload the TLS traffic from the load balancer, inspect it for threats, and then forward it to your web application.

This method ensures that incoming traffic is thoroughly inspected for malware and other threats before reaching your application, providing a secure environment.

👍 ↩️ 🚩 upvoted 2 times

🗄️  **YourFriendlyNeighborhoodSpider** 4 months, 1 week ago

This is not true. Google Cloud does not offer a native Secure Web Proxy with TLS interception for incoming traffic. Load balancers in Google Cloud do not provide deep TLS interception for security inspection.

👍 ↩️ 🚩 upvoted 1 times

🗄️  **JohnDohertyDoe** 7 months ago

Selected Answer: C

C is the right answer, you cannot enable TLS inspection for a simple firewall rule. You would need to add it to a Hierarchical Policy or a Global Firewall policy.

👍 ↩️ 🚩 upvoted 1 times


🗄️  **Zek** 7 months, 3 weeks ago

Selected Answer: C

<https://cloud.google.com/firewall/docs/about-firewalls>

Cloud NGFW implements network and hierarchical firewall policies that can be attached to a resource hierarchy node. These policies provide a consistent firewall experience across the Google Cloud resource hierarchy.

👍 ↩️ 🚩 upvoted 1 times

🗄️  **Pime13** 7 months, 3 weeks ago

Selected Answer: A

<https://cloud.google.com/secure-web-proxy/docs/tls-inspection-overview>

Secure Web Proxy provides a TLS inspection service that allows you to intercept, inspect, and enforce security policies on TLS traffic. This approach ensures that incoming traffic is thoroughly inspected for threats before reaching your application.

👍 ↩️ 🚩 upvoted 1 times

🗄️  **BPzen** 8 months ago

Selected Answer: C

Why C is Correct:

Hierarchical Firewall Policy:

A hierarchical firewall policy allows you to enforce consistent firewall rules across an organization, folders, or projects.

Configuring TLS interception within this policy ensures that all relevant traffic passing through the policy can be decrypted, inspected, and then forwarded.

A. Configure Secure Web Proxy. Offload the TLS traffic in the load balancer, inspect the traffic, and forward the traffic to the web application.

web application.

Secure Web Proxy is not designed to handle incoming traffic for web applications in Google Cloud; it is typically used for outbound traffic filtering.

This approach would not address the requirement to protect incoming traffic with TLS interception.

👍 ↩ 🚩 upvoted 1 times

🗄️ 👤 **MoAk** 8 months ago

Selected Answer: C

<https://cloud.google.com/firewall/docs/about-tls-inspection>

👍 ↩ 🚩 upvoted 2 times

🗄️ 👤 **KLei** 8 months, 2 weeks ago

Selected Answer: A

Secure Web Proxy: This setup allows you to intercept and inspect TLS traffic securely. By configuring a Secure Web Proxy, you can manage incoming traffic more effectively and implement security measures against threats.

TLS Offloading at the Load Balancer: By offloading TLS traffic at the load balancer, you can decrypt and inspect the traffic before forwarding it to your web application.

👍 ↩ 🚩 upvoted 1 times

🗄️ 👤 **KLei** 8 months, 2 weeks ago

Sorry, seems D is better as secure web proxy is for outgoing traffic while next gen firewall is for both incoming and outgoing traffic.

👍 ↩ 🚩 upvoted 1 times

🗄️ 👤 **junb** 9 months, 1 week ago

C is Correct

👍 ↩ 🚩 upvoted 1 times

🗄️ 👤 **BB_norway** 10 months, 1 week ago

Selected Answer: D

With the Enterprise tier we can intercept TLS traffic

👍 ↩ 🚩 upvoted 3 times

🗄️ 👤 **json4u** 9 months, 2 weeks ago

Ofcourse it's D.

Secure Web Proxy primarily handles outbound (egress) web traffic.

Next Generation Firewall (NGFW) Enterprise supports TLS interception also, and it's a better fit for this scenario involving traffic protection for a web application accessed from an on-premises network.

👍 ↩ 🚩 upvoted 2 times

🗄️ 👤 **ABotha** 10 months, 3 weeks ago

B is correct. Secure Web Proxy is typically used for external traffic, not internal traffic from an on-premises network.

👍 ↩ 🚩 upvoted 2 times

🗄️ 👤 **Pach1211** 10 months, 2 weeks ago

An internal proxy load balancer is designed for load balancing within the Google Cloud environment and is not suitable for intercepting and inspecting TLS traffic from external sources, such as traffic coming from an on-premises network to a web application hosted on Google Cloud.

👍 ↩ 🚩 upvoted 1 times

🗄️ 👤 **yokoyan** 10 months, 3 weeks ago

Selected Answer: A

I think it's A.

👍 ↩ 🚩 upvoted 2 times



Platform

> Home

> All Exams

> Examtopics PRO

> Training Courses



© 2024 ExamTopics