

[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 64 DISCUSSION

Actual exam question from Google's Professional Cloud Security Engineer

Question #: 64

Topic #: 1

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

In an effort for your company messaging app to comply with FIPS 140-2, a decision was made to use GCP compute and network services. The messaging app architecture includes a Managed Instance Group (MIG) that controls a cluster of Compute Engine instances. The instances use Local SSDs for data caching and UDP for instance-to-instance communications. The app development team is willing to make any changes necessary to comply with the standard

Which options should you recommend to meet the requirements?


- A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.
- B. Set Disk Encryption on the Instance Template used by the MIG to customer-managed key and use BoringSSL for all data transit between instances.
- C. Change the app instance-to-instance communications from UDP to TCP and enable BoringSSL on clients' TLS connections.
- D. Set Disk Encryption on the Instance Template used by the MIG to Google-managed Key and use BoringSSL library on all instance-to-instance communications.

[Show Suggested Answer](#)

by  MohitA at Sept. 2, 2020, 9:55 a.m.

## Comments

Submit

  **subhala** Highly Voted 4 years, 8 months ago

when I revisited this, Now I think A is correct. In A - We will use an approved encryption method for encrypting Local SSD and VM to VM communication. In B and D, we are still using GCP's encryption algorithms and are not FIPS 140-2 approved. Moreover only the BoringCrypto is FIPS 140-2 approved and not the Boring SSL. I see A as evidently correct. ownez, genesis3k, MohitA has explained this and provided the right links too.

   upvoted 16 times



  **Rakesh21** Most Recent 5 months, 4 weeks ago

Selected Answer: B

Disk Encryption with customer-managed keys: FIPS 140-2 compliance often requires encryption, and using customer-managed encryption keys (CMEK) ensures that you have control over the encryption keys, which can be crucial for compliance. Google Cloud supports FIPS 140-2 compliant encryption for data at rest with customer-managed keys.

BoringSSL for data transit: BoringSSL is Google's fork of OpenSSL, designed to meet high standards of cryptographic security, including FIPS 140-2. Using BoringSSL for instance-to-instance communications ensures that data in transit is encrypted according to the necessary standards. Although UDP isn't inherently encrypted, you can implement encryption at the application layer using libraries like BoringSSL.

   upvoted 1 times

  **p981pa123** 6 months ago

Selected Answer: A

"BoringSSL as a whole is not FIPS validated. However, there is a core library (called BoringCrypto) that has been FIPS validated."



   upvoted 2 times

  **p981pa123** 6 months, 2 weeks ago

Selected Answer: B

When you deploy Managed Instance Groups (MIGs), you typically create an instance template that defines the configuration of instances in the group, including the disk encryption settings.

   upvoted 1 times

  **p981pa123** 6 months ago

I made mistake . Answer is A.

"BoringSSL as a whole is not FIPS validated. However, there is a core library (called BoringCrypto) that has been FIPS validated."

<https://boringssl.googlesource.com/boringssl/+master/crypto/fipsmodule/FIPS.md>

   upvoted 1 times

  **SQLbox** 10 months, 2 weeks ago

B

To comply with FIPS 140-2, the company needs to ensure that both data at rest and data in transit are encrypted using cryptographic libraries that are FIPS 140-2 certified.




- Customer-managed keys (CMEK): Using customer-managed encryption keys (CMEK) in Google Cloud Key Management Service (KMS) ensures that encryption complies with FIPS 140-2 standards because the customer has control over the encryption keys and can ensure they are managed according to compliance requirements.
- BoringSSL: A Google-maintained version of OpenSSL designed to be more streamlined and used in environments like Google Cloud, which includes support for FIPS 140-2 mode when linked to the BoringCrypto module. This library can be used to ensure that data in transit between instances is encrypted in compliance with FIPS.

   upvoted 1 times

  **LaithTech** 11 months, 3 weeks ago

Selected Answer: B

The correct answer is B

   upvoted 1 times

  **3d9563b** 1 year ago

Selected Answer: B

A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module:

BoringCrypto is not an established or widely recognized cryptographic library for FIPS 140-2 compliance. Instead, BoringSSL or OpenSSL with FIPS validation should be used for both data-at-rest and data-in-transit encryption.



C. Change the app instance-to-instance communications from UDP to TCP and enable BoringSSL on clients' TLS connections:

While changing from UDP to TCP might provide more reliable connections, it does not directly address FIPS 140-2 compliance. You still need to ensure that all data-in-transit encryption uses a validated cryptographic module such as BoringSSL.

D. Set Disk Encryption on the Instance Template used by the MIG to Google-managed Key and use BoringSSL library on all instance-to-instance communications:

Google-managed keys for disk encryption do not provide the level of control required for FIPS 140-2 compliance, which typically requires customer-managed keys for greater control and accountability.

   upvoted 1 times

  **gical** 1 year, 7 months ago

Selected answer B

<https://cloud.google.com/security/compliance/fips-140-2-validated/>

"Google's Local SSD storage product is automatically encrypted with NIST approved ciphers, but Google's current implementation for this product doesn't have a FIPS 140-2 validation certificate. If you require FIPS-validated encryption on Local SSD storage, you must provide your own encryption with a FIPS-validated cryptographic module."

   upvoted 4 times

  **b6f53d8** 1 year, 6 months ago

YES, as in your link: you need to encrypt SSD using your own solution, and BoringSSL is a library to use

   upvoted 1 times

  **ArizonaClassics** 1 year, 10 months ago

A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.

This option ensures both storage (Local SSDs) and inter-instance communications are encrypted using a FIPS 140-2 compliant module.


   upvoted 4 times

  **ArizonaClassics** 1 year, 10 months ago

A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.

This option ensures both storage (Local SSDs) and inter-instance communications are encrypted using a FIPS 140-2 compliant module.

   upvoted 1 times

  **ymkk** 1 year, 10 months ago

Selected Answer: A

<https://cloud.google.com/security/compliance/fips-140-2-validated/>

   upvoted 2 times

  **gcpengineer** 2 years, 2 months ago

Selected Answer: A

A is the ans

   upvoted 2 times

  **pedrojorge** 2 years, 6 months ago

Selected Answer: C

"BoringSSL as a whole is not FIPS validated. However, there is a core library (called BoringCrypto) that has been FIPS validated"

<https://boringssl.googlesource.com/boringssl/+/-/master/crypto/fipsmodule/FIPS.md>


   upvoted 3 times

  **AzureDP900** 2 years, 8 months ago

<https://cloud.google.com/docs/security/key-management-deep-dive>


A is right

   upvoted 1 times

  **AwesomeGCP** 2 years, 9 months ago

Selected Answer: A

A. Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.

   upvoted 1 times

  **sudarchary** 3 years, 5 months ago

Selected Answer: A

FIPS140 module is supported

   upvoted 2 times

  **DehasichI nwas** 4 years, 4 months ago

— Discussion 1 year, 1 month ago

Ans : A

   upvoted 1 times

[Load full discussion...](#)



## Platform

> [Home](#)

> [Examtopics PRO](#)

> [All Exams](#)

> [Training Courses](#)



© 2024 ExamTopics