PROFESSIONAL-CLOUD-SECURITY-ENGINEER$^{Q\&As}$

Professional Cloud Security Engineer

Pass Google PROFESSIONAL-CLOUD-SECURITY-ENGINEER Exam with 100% Guarantee

Following Questions and Answers are all new published by Google Official Exam Center

QUESTION 1

Your organization\\'s Google Cloud VMs are deployed via an instance template that configures them with a public IP address in order to host web services for external users. The VMs reside in a service project that is attached to a host (VPC) project containing one custom Shared VPC for the VMs. You have been asked to reduce the exposure of the VMs to the internet while continuing to service external users. You have already recreated the instance template without a public IP address configuration to launch the managed instance group (MIG). What should you do?

A. Deploy a Cloud NAT Gateway in the service project for the MIG.

B. Deploy a Cloud NAT Gateway in the host (VPC) project for the MIG.

C. Deploy an external HTTP(S) load balancer in the service project with the MIG as a backend.

D. Deploy an external HTTP(S) load balancer in the host (VPC) project with the MIG as a backend.

Correct Answer: C

QUESTION 2

A customer\\'s internal security team must manage its own encryption keys for encrypting data on Cloud Storage and decides to use customer-supplied encryption keys (CSEK).

How should the team complete this task?

A. Upload the encryption key to a Cloud Storage bucket, and then upload the object to the same bucket.

B. Use the gsutil command line tool to upload the object to Cloud Storage, and specify the location of the encryption key.

C. Generate an encryption key in the Google Cloud Platform Console, and upload an object to Cloud Storage using the specified key.

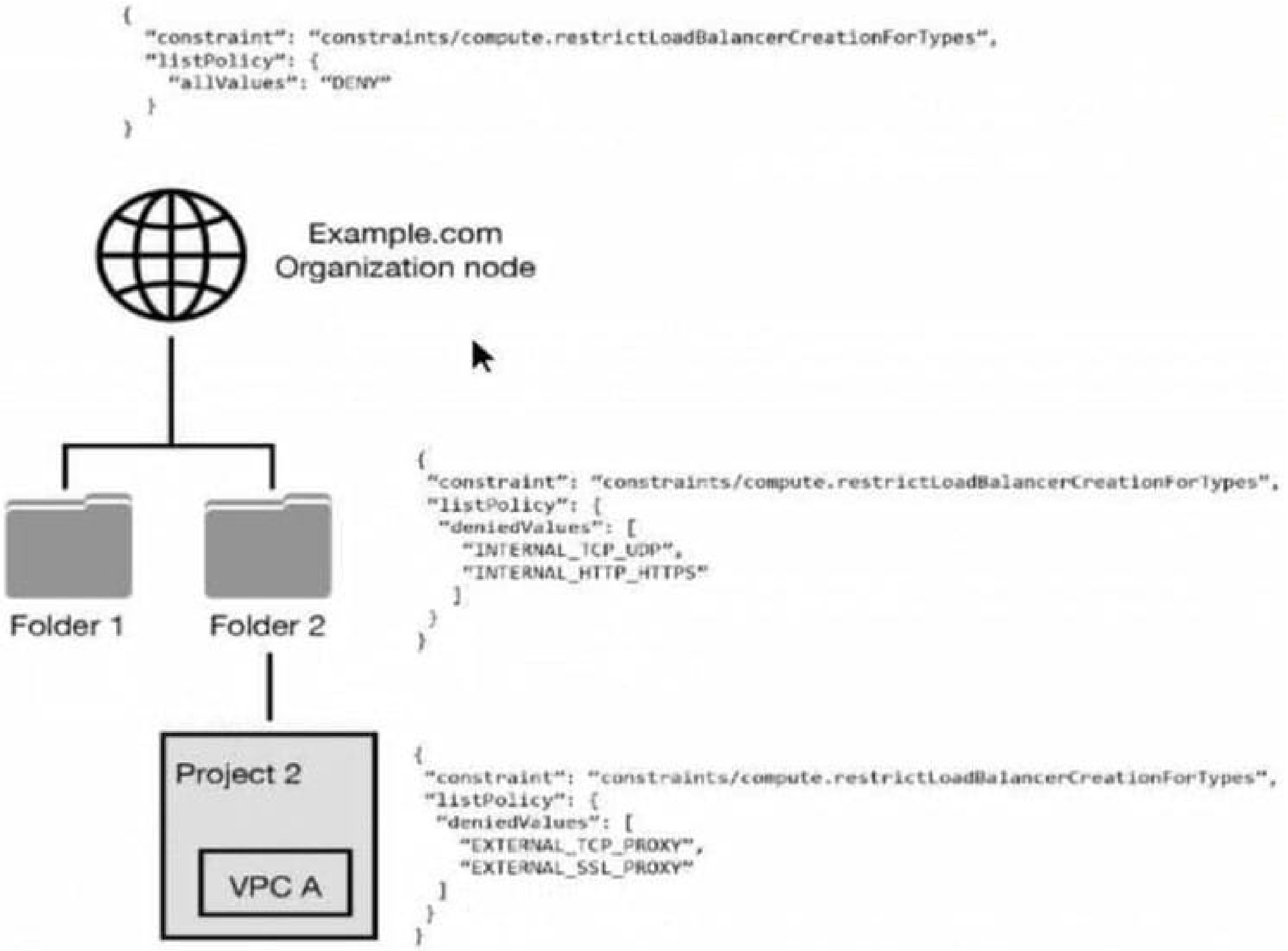
D. Encrypt the object, then use the gsutil command line tool or the Google Cloud Platform Console to upload the object to Cloud Storage.

Correct Answer: B

https://cloud.google.com/storage/docs/encryption/customer-supplied-keys#gsutil

QUESTION 3

You have the following resource hierarchy. There is an organization policy at each node in the hierarchy as shown. Which load balancer types are denied in VPC A?



```
{
  “constraint”: “constraints/compute.restrictLoadBalancerCreationForTypes”,
  “listPolicy”: {
    “allValues”: “DENY”
  }
}
```

```
{
 “constraint”: “constraints/compute.restrictLoadBalancerCreationForTypes”,
 “listPolicy”: {
  “deniedValues”: [
    “INTERNAL_TCP_UDP”,
    “INTERNAL_HTTP_HTTPS”
  ]
 }
}
```

```
{
 “constraint”: “constraints/compute.restrictLoadBalancerCreationForTypes”,
 “listPolicy”: {
  “deniedValues”: [
    “EXTERNAL_TCP_PROXY”,
    “EXTERNAL_SSL_PROXY”
  ]
 }
}
```

A. All load balancer types are denied in accordance with the global node\\'s policy.

B. INTERNAL_TCP_UDP, INTERNAL_HTTP_HTTPS is denied in accordance with the folder\\'s policy.

C. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY are denied in accordance with the project\\'s policy.

D. EXTERNAL_TCP_PROXY, EXTERNAL_SSL_PROXY, INTERNAL_TCP_UDP, and INTERNAL_HTTP_HTTPS are denied in accordance with the folder and project\\'s policies.

Correct Answer: A

QUESTION 4

Your team wants to limit users with administrative privileges at the organization level. Which two roles should your team restrict? (Choose two.)

A. Organization Administrator

B. Super Admin

C. GKE Cluster Admin

D. Compute Admin

E. Organization Role Viewer

Correct Answer: AB

Reference: https://cloud.google.com/resource-manager/docs/creating-managing-organization

QUESTION 5

A customer needs to prevent attackers from hijacking their domain/IP and redirecting users to a malicious site through a man-in-the-middle attack.

Which solution should this customer use?

A. VPC Flow Logs

B. Cloud Armor

C. DNS Security Extensions

D. Cloud Identity-Aware Proxy

Correct Answer: C

Reference: https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns DNSSEC --use a DNS registrar that supports DNSSEC, and enable it. DNSSEC digitally signs DNS communication, making it more difficult (but not impossible) for hackers to intercept and spoof. Domain Name System Security Extensions (DNSSEC) adds security to the Domain Name System (DNS) protocol by enabling DNS responses to be validated. Having a trustworthy Domain Name System (DNS) that translates a domain name like www.example.com into its associated IP address is an increasingly important building block of today\\'s web-based applications. Attackers can hijack this process of domain/IP lookup and redirect users to a malicious site through DNS hijacking and man-in-the-middle attacks. DNSSEC helps mitigate the risk of such attacks by cryptographically signing DNS records. As a result, it prevents attackers from issuing fake DNS responses that may misdirect browsers to nefarious websites. https://cloud.google.com/blog/products/gcp/dnssec-now-available-in-cloud-dns