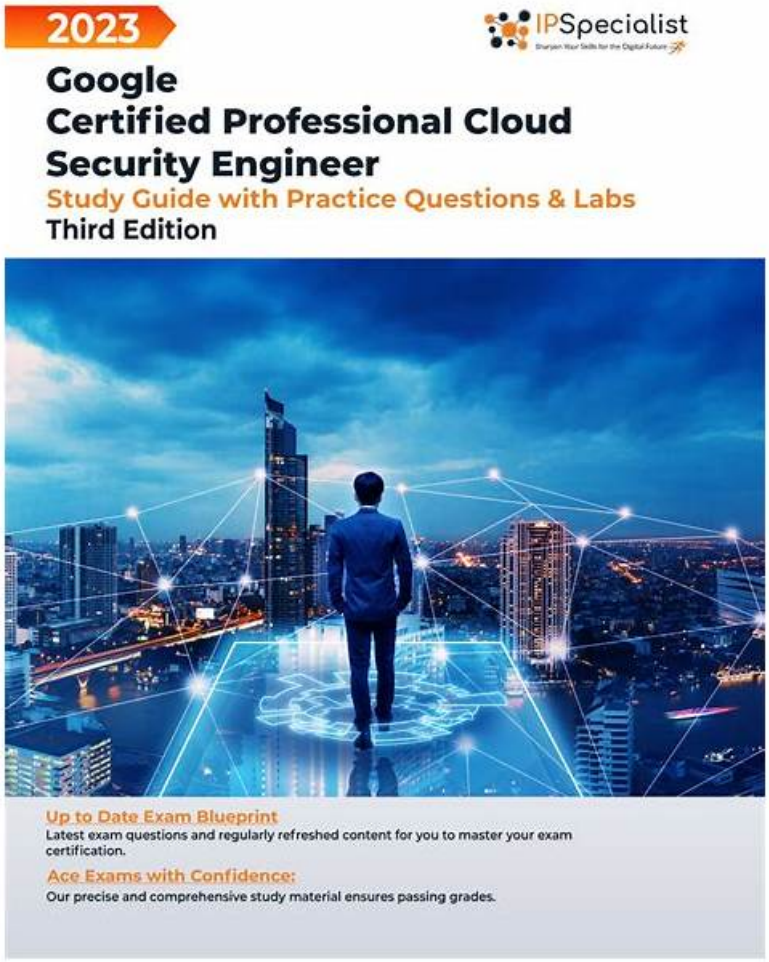
# Top Features of Itcertkey Google Professional-Cloud-Security-Engineer Exam Questions




2026 Latest Itcertkey Professional-Cloud-Security-Engineer PDF Dumps and Professional-Cloud-Security-Engineer Exam Engine Free Share: https://drive.google.com/open?id=1lHvypA5V-vDSaFseVqaTlcTeUxDk1-jZ

The Google Professional-Cloud-Security-Engineer is a very prestigious certificate that is considered a guarantee of a well-paid job in a reputed tech firm. Most candidates attempting the Google Cloud Certified - Professional Cloud Security Engineer Exam test are nervous. Very few applicants can earn the Google Cloud Certified - Professional Cloud Security Engineer Exam Professional-Cloud-Security-Engineer certificate on their first attempts because of the challenging level of topics included in the Google Professional-Cloud-Security-Engineer test. Itcertkey Professional-Cloud-Security-Engineer actual dumps help applicants in clearing the test very easily.

The Google Professional Cloud Security Engineer exam is targeted towards IT professionals who are responsible for designing and implementing secure infrastructures on the Google Cloud Platform. Through mastery of industry-specific security requirements, accredited individuals will demonstrate their competency in designing, developing, and managing secure infrastructure using Google security technologies.

## There are 3 study programs available that you can use to prepare for the test. Also, Google provides tons of skill badges that you can complete to verify your competence in implementing cloud security concepts at this level. We will be covering all of them below:

**1. Google Cloud Fundamentals: Core Infrastructure**

This course will help you build an important foundation for working with popular computing and storage devices in Google Cloud efficiently. These include Google Kubernetes, Cloud SQL, Cloud Storage, BigQuery, App Engine, and Compute Engine. Besides, this training option will also provide important coverage of resource and policy management tools such as Cloud Identity and Access Management and the Resource Manager hierarchy. If you are experienced in working with Azure or AWS and now looking to switch to Google Cloud, this course will be the best tool to ease the transition.

**>> Professional-Cloud-Security-Engineer Reliable Exam Braindumps <<**

## Reliable Google Professional-Cloud-Security-Engineer Test Book - New Professional-Cloud-Security-Engineer Real Exam

In recent years, some changes are taking place in this line about the new points are being constantly tested in the Professional-Cloud-Security-Engineer real exam. So our experts highlights the new type of questions and add updates into the Professional-Cloud-Security-Engineer practice materials, and look for shifts closely when them take place. At the same time, as we can see that the electronic devices are changing our life day by day, our Professional-Cloud-Security-Engineer study questions are also developed to apply all kinds of eletronic devices.

Google Professional-Cloud-Security-Engineer exam is a certification provided by Google Cloud that is aimed at professionals who want to master the complex world of cloud security. Google Cloud Certified - Professional Cloud Security Engineer Exam certification is designed to validate the skills and knowledge required to implement and manage security solutions in the Google Cloud Platform. Professional-Cloud-Security-Engineer Exam covers a wide range of topics, including network security, application security, data encryption, identity and access management, and security operations. Professional-Cloud-Security-Engineer exam follows a scenario-based format and tests the candidate's ability to identify security risks, design and implement security solutions, and monitor and manage security incidents.

## Google Cloud Certified - Professional Cloud Security Engineer Exam Sample Questions (Q119-Q124):

**NEW QUESTION # 119**
Your organization uses Google Workspace Enterprise Edition for authentication. You are concerned about employees leaving their laptops unattended for extended periods of time after authenticating into Google Cloud. You must prevent malicious people from using an employee's unattended laptop to modify their environment.
What should you do?

- A. Set the session length timeout for Google Cloud services to a shorter duration.
- B. Require strong passwords and 2SV through a security token or Google authenticator.
- C. Review and disable unnecessary Google Cloud APIs.
- D. Create a policy that requires employees to not leave their sessions open for long durations.

**Answer: A**

**NEW QUESTION # 120**
You have numerous private virtual machines on Google Cloud. You occasionally need to manage the servers through Secure Socket Shell (SSH) from a remote location. You want to configure remote access to the servers in a manner that optimizes security and cost efficiency.
What should you do?

- A. Create a firewall rule to allow access from the Identity-Aware Proxy (IAP) IP range. Grant the role of an IAP-secured Tunnel User to the administrators.
- B. Create a jump host instance with public IP. Manage the instances by connecting through the jump host.
- C. Create a site-to-site VPN from your corporate network to Google Cloud.
- D. Configure server instances with public IP addresses. Create a firewall rule to only allow traffic from your corporate IPs.

**Answer: A**

Explanation:
With TCP forwarding, IAP can protect SSH and RDP access to your VMs hosted on Google Cloud. Your VM instances don't even need public IP addresses.

https://cloud.google.com/iap#section-2

**NEW QUESTION # 121**
A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The customer's internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection.
Which product should be used to meet these requirements?

- A. Cloud CDN
- B. Cloud Identity and Access Management
- C. Cloud Armor
- D. VPC Firewall Rules

**Answer: C**

**NEW QUESTION # 122**
Your organization hosts a financial services application running on Compute Engine instances for a third-party company. The third-party company's servers that will consume the application also run on Compute Engine in a separate Google Cloud organization.
You need to configure a secure network connection between the Compute Engine instances. You have the following requirements:
The network connection must be encrypted.
The communication between servers must be over private IP addresses.
What should you do?

- A. Configure a Cloud VPN connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.
- B. Configure a VPC peering connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.
- C. Configure an Apigee proxy that exposes your Compute Engine-hosted application as an API, and is encrypted with TLS which allows access only to the third party.
- D. Configure a VPC Service Controls perimeter around your Compute Engine instances, and provide access to the third party via an access level.

**Answer: A**

Explanation:
To meet the requirements of encrypted communication over private IP addresses between Compute Engine instances in different Google Cloud organizations, a Cloud VPN connection is appropriate:
Cloud VPN: Cloud VPN creates a secure, encrypted tunnel between your organization's VPC network and the third party's VPC network. This ensures that data transmitted over the network is encrypted and secure.
Private IP Communication: Cloud VPN allows communication over private IP addresses, which helps maintain security by keeping traffic within the Google Cloud network and not exposing it to the public internet.
Firewall Rules: VPC firewall rules can be configured to control the traffic that flows through the VPN, ensuring that only authorized traffic is allowed, further enhancing security.
By setting up a Cloud VPN connection, you can achieve secure, encrypted communication over private IP addresses between different Google Cloud organizations.
Reference:
Cloud VPN Overview

**NEW QUESTION # 123**
You are a Cloud Identity administrator for your organization. In your Google Cloud environment, groups are used to manage user permissions. Each application team has a dedicated group.
Your team is responsible for creating these groups and the application teams can manage the team members on their own through the Google Cloud console. You must ensure that the application teams can only add users from within your organization to their groups.
What should you do?

- A. Export the Cloud Identity logs to BigQuery. Configure an alert for external members added to groups. Have the alert trigger a Cloud Function instance that removes the external members from the group.
- B. Set an Identity and Access Management (IAM) policy that includes a condition that restricts group membership to user principals that belong to your organization.
- C. Define an Identity and Access Management (IAM) deny policy that denies the assignment of principals that are outside your organization to the groups in scope.
- D. Change the configuration of the relevant groups in the Google Workspace Admin console to prevent external users from being added to the group.

**Answer: D**

Explanation:
https://support.google.com/a/answer/167097?hl=en&sjid=9952232817978914605-AP

**NEW QUESTION # 124**
.....

myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.wcs.edu.eu, www.stes.tyc.edu.tw, Disposable vapes

P.S. Free & New Professional-Cloud-Security-Engineer dumps are available on Google Drive shared by Itcertkey: https://drive.google.com/open?id=1lHvypA5V-vDSaFseVqaTlcTeUxDk1-jZ