Google Cloud

Partner Certification Academy

Professional Cloud Developer

v2309

Quiz questions: Cloud IAP*

** These are for practice only and are not actual exam questions*

What is the primary purpose of Identity-Aware Proxy (IAP) in Google Cloud?

a. To manage network-level firewalls
b. To centralize authorization for HTTPS applications
c. To secure internal HTTP traffic
d. To provide VPN access to resources

When should you use IAP in Google Cloud?

a. When you need to protect activity within a project
b. When you want to secure access only to Cloud Run

c. When you require VPN access to your applications
d. When you want to enforce access control policies for applications and resources

How does IAP determine if a user is authorized to access a protected resource?

a. By checking the user's browser history
a. By verifying the user's VPN connection
b. By performing authentication and applying IAM policies
c. By inspecting the user's device type

In which scenario can users bypass IAP authentication?

a. When accessing the application-serving port of a Compute Engine VM
b. When using Cloud Run with proper ingress controls
c. When accessing resources through HTTPS load balancing
d. When they have the IAP-secured Web App User role

What is one of the responsibilities you should consider when using IAP?

a. Managing firewall and load balancer configurations to protect traffic
b. Configuring OAuth 2.0 client ID and secret for IAP
c. Synchronizing Google Accounts with Active Directory
d. Managing internal HTTP load balancer

Answers:

What is the primary purpose of Identity-Aware Proxy (IAP) in Google Cloud?

b) To centralize authorization for HTTPS applications. IAP lets you establish a central authorization layer for applications accessed by HTTPS, so you can use an application-level access control model instead of relying on network-level firewalls.
https://cloud.google.com/iap/docs/concepts-overview

When should you use IAP in Google Cloud?

d) When you want to enforce access control policies for applications and resources.
https://cloud.google.com/iap/docs/concepts-overview

How does IAP determine if a user is authorized to access a protected resource?

c) By performing authentication and applying IAM policies. After authentication, IAP applies the relevant IAM policy to check if the user is authorized to access the requested resource. If the user has the IAP-secured Web App User role on the Google Cloud console project where the resource exists, they're authorized to access the application.
https://cloud.google.com/iap/docs/concepts-overview

In which scenario can users bypass IAP authentication?

a) When accessing the application-serving port of a Compute Engine VM.If you're using Compute Engine or Google Kubernetes Engine, users who can access the application-serving port of the Virtual Machine (VM) can bypass IAP authentication. Compute Engine and GKE firewall rules can't protect against access from code running on the same VM as the IAP-secured application. Firewall rules can protect against access from another VM, but only if properly configured.
https://cloud.google.com/iap/docs/concepts-overview
https://cloud.google.com/compute/docs/authentication

What is one of the responsibilities you should consider when using IAP?

a) Managing firewall and load balancer configurations to protect traffic. IAP secures authentication and authorization of all requests to App Engine, Cloud Load Balancing (HTTPS), or internal HTTP load balancing. IAP doesn't protect against activity within a project, such as another VM inside the project.
https://cloud.google.com/iap/docs/concepts-overview
https://cloud.google.com/iap/docs/load-balancer-howto