PROFESSIONAL-CLOUD-SECURITY-ENGINEER Q&As

Professional Cloud Security Engineer

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

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/professional-cloud-security-engineer.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You control network traffic for a folder in your Google Cloud environment. Your folder includes multiple projects and Virtual Private Cloud (VPC) networks. You want to enforce on the folder level that egress connections are limited only to IP range 10.58.5.0/24 and only from the VPC network "dev-vpc". You want to minimize implementation and maintenance effort.

What should you do?

A. 1. Leave the network configuration of the VMs in scope unchanged.

2.

Create a new project including a new VPC network "new-vpc".

3.

Deploy a network appliance in "new-vpc" to filter access requests and only allow egress connections from "dev-vpc" to 10.58.5.0/24.

B. 1. Leave the network configuration of the VMs in scope unchanged.

2. Enable Cloud NAT for "dev-vpc" and restrict the target range in Cloud NAT to 10.58.5.0/24.

C. 1. Attach external IP addresses to the VMs in scope.

2. Define and apply a hierarchical firewall policy on folder level to deny all egress connections and to allow egress to IP range 10.58.5.0/24 from network dev-vpc.

D. 1. Attach external IP addresses to the VMs in scope.

2. Configure a VPC Firewall rule in "dev-vpc" that allows egress connectivity to IP range 10.58.5.0/24 for all source addresses in this network.

Correct Answer: C

The correct answer is C. 1. Attach external IP addresses to the VMs in scope. 2. Define and apply a hierarchical firewall policy on folder level to deny all egress connections and to allow egress to IP range 10.58.5.0/24 from network dev-vpc.

This approach allows you to control network traffic at the folder level. By attaching external IP addresses to the VMs in scope, you can ensure that the VMs have a unique, routable IP address for outbound connections. Then, by defining and applying a hierarchical firewall policy at the folder level, you can enforce that egress connections are limited to the specified IP range and only from the specified VPC network.

QUESTION 2

Which two security characteristics are related to the use of VPC peering to connect two VPC networks? (Choose two.)

A. Central management of routes, firewalls, and VPNs for peered networks

B. Non-transitive peered networks; where only directly peered networks can communicate

C. Ability to peer networks that belong to different Google Cloud Platform organizations

D. Firewall rules that can be created with a tag from one peered network to another peered network

E. Ability to share specific subnets across peered networks

Correct Answer: BC

https://cloud.google.com/vpc/docs/vpc-peering#key_properties

QUESTION 3

An engineering team is launching a web application that will be public on the internet. The web application is hosted in multiple GCP regions and will be directed to the respective backend based on the URL request.

Your team wants to avoid exposing the application directly on the internet and wants to deny traffic from a specific list of malicious IP addresses

Which solution should your team implement to meet these requirements?

A. Cloud Armor

B. Network Load Balancing

C. SSL Proxy Load Balancing

D. NAT Gateway

Correct Answer: A

https://cloud.google.com/armor/docs/security-policy-overview#edge-security Reference: https://cloud.google.com/armor/docs/security-policy-concepts

QUESTION 4

As part of your organization\\'s zero trust strategy, you use Identity-Aware Proxy (IAP) to protect multiple applications. You need to ingest logs into a Security Information and Event Management (SIEM) system so that you are alerted to possible intrusions.

Which logs should you analyze?

A. Data Access audit logs

B. Policy Denied audit logs

C. Cloud Identity user log events

D. Admin Activity audit logs

Correct Answer: A

The data_access log name only appears if there was traffic to your resource after you enabled Cloud Audit Logs for IAP.

Click to expand the date and time of the access you want to review.

Authorized access has a blue i icon. Unauthorized access has an orange !! icon. "

https://cloud.google.com/iap/docs/audit-log-howto

QUESTION 5

Your team wants to centrally manage GCP IAM permissions from their on-premises Active Directory Service. Your team wants to manage permissions by AD group membership.

What should your team do to meet these requirements?

A. Set up Cloud Directory Sync to sync groups, and set IAM permissions on the groups.

B. Set up SAML 2.0 Single Sign-On (SSO), and assign IAM permissions to the groups.

C. Use the Cloud Identity and Access Management API to create groups and IAM permissions from Active Directory.

D. Use the Admin SDK to create groups and assign IAM permissions from Active Directory.

Correct Answer: A

"In order to be able to keep using the existing identity management system, identities need to be synchronized between AD and GCP IAM. To do so google provides a tool called Cloud Directory Sync. This tool will read all identities in AD and replicate those within GCP. Once the identities have been replicated then it\\'s possible to apply IAM permissions on the groups. After that you will configure SAML so google can act as a service provider and either you ADFS or other third party tools like Ping or Okta will act as the identity provider. This way you effectively delegate the authentication from Google to something that is under your control."

QUESTION 6

You are creating a new infrastructure CI/CD pipeline to deploy hundreds of ephemeral projects in your Google Cloud organization to enable your users to interact with Google Cloud. You want to restrict the use of the default networks in your organization while following Google-recommended best practices. What should you do?

A. Enable the constraints/compute.skipDefaultNetworkCreation organization policy constraint at the organization level.

B. Create a cron job to trigger a daily Cloud Function to automatically delete all default networks for each project.

C. Grant your users the 1AM Owner role at the organization level. Create a VPC Service Controls perimeter around the project that restricts the compute.googleapis.com API.

D. Only allow your users to use your CI/CD pipeline with a predefined set of infrastructure templates they can deploy to skip the creation of the default networks.

Correct Answer: A

Enable the constraints/compute.skipDefaultNetworkCreation organization policy constraint at the organization level.
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints-constraints/compute.skipDefaultNetworkCreation

This boolean constraint skips the creation of the default network and related resources during Google Cloud Platform

Project resource creation where this constraint is set to True. By default, a default network and supporting resources are automatically created when creating a Project resource.

QUESTION 7

You are migrating your users to Google Cloud. There are cookie replay attacks with Google web and Google Cloud CLI SDK sessions on endpoint devices. You need to reduce the risk of these threats. What should you do? (Choose two.)

A. Configure Google session control to a shorter duration.

B. Set an organizational policy for OAuth 2.0 access token with a shorter duration.

C. Set a reauthentication policy for Google Cloud services to a shorter duration.

D. Configure a third-party identity provider with session management.

E. Enforce Security Key Authentication with 2SV.

Correct Answer: AE

Correct anwers are A and E.

A. Configuring Google session control to a shorter duration reduces the time window in which an attacker can use a replayed cookie to gain unauthorized access, thereby enhancing security.

E. Enforcing Security Key Authentication with 2-Step Verification (2SV) adds an additional layer of security by requiring users to verify their identity using a physical security key, making it more difficult for attackers to gain unauthorized access even if they have a replayed cookie.

QUESTION 8

Your company is using Cloud Dataproc for its Spark and Hadoop jobs. You want to be able to create, rotate, and destroy symmetric encryption keys used for the persistent disks used by Cloud Dataproc. Keys can be stored in the cloud.

What should you do?

A. Use the Cloud Key Management Service to manage the data encryption key (DEK).

B. Use the Cloud Key Management Service to manage the key encryption key (KEK).

C. Use customer-supplied encryption keys to manage the data encryption key (DEK).

D. Use customer-supplied encryption keys to manage the key encryption key (KEK).

Correct Answer: B

This PD and bucket data is encrypted using a Google-generated data encryption key (DEK) and key encryption key (KEK). The CMEK feature allows you to create, use, and revoke the key encryption key (KEK). Google still controls the data encryption key (DEK). For more information on Google data encryption keys, see Encryption at Rest.

https://cloud.google.com/dataproc/docs/concepts/configuring-clusters/customer-managed-encryption
https://codelabs.developers.google.com/codelabs/encrypt-and-decrypt-data-with-cloud-kms#0

QUESTION 9

Your organization is using Active Directory and wants to configure Security Assertion Markup Language (SAML). You must set up and enforce single sign-on (SSO) for all users.

What should you do?

A. 1. Create a new SAML profile.

2.

Populate the sign-in and sign-out page URLs.

3.

Upload the X.509 certificate.

4.

Configure Entity ID and ACS URL in your IdP.

B. 1. Configure prerequisites for OpenID Connect (OIDC) in your Active Directory (AD) tenant.

2.

Verify the AD domain.

3.

Decide which users should use SAML.

4.

Assign the pre-configured profile to the select organizational units (OUs) and groups.

C. 1. Create a new SAML profile.

2.

Upload the X.509 certificate.

3.

Enable the change password URL.

4.

Configure Entity ID and ACS URL in your IdP.

D. 1. Manage SAML profile assignments.

2.

Enable OpenID Connect (OIDC) in your Active Directory (AD) tenant.

3.

Verify the domain.

Correct Answer: A

When configuring SAML-based Single Sign-On (SSO) in an organization that\\'s using Active Directory, the general steps would involve setting up a SAML profile, specifying the necessary URLs for sign-in and sign- out processes, uploading an X.509 certificate for secure communication, and setting up the Entity ID and Assertion Consumer Service (ACS) URL in the Identity Provider (which in this case would be Active Directory).

A. Create a new SAML profile, populate URLs, upload X.509 certificate, configure Entity ID and ACS URL: This option comprehensively covers the steps necessary for setting up SAML-based SSO.

QUESTION 10

You are implementing data protection by design and in accordance with GDPR requirements. As part of design reviews, you are told that you need to manage the encryption key for a solution that includes workloads for Compute Engine,

Google Kubernetes Engine, Cloud Storage, BigQuery, and Pub/Sub.

Which option should you choose for this implementation?

A. Cloud External Key Manager

B. Customer-managed encryption keys

C. Customer-supplied encryption keys

D. Google default encryption

Correct Answer: A

QUESTION 11

You need to connect your organization\\'s on-premises network with an existing Google Cloud environment that includes one Shared VPC with two subnets named Production and Non-Production. You are required

to:

Use a private transport link.

Configure access to Google Cloud APIs through private API endpoints originating from on-premises environments.

Ensure that Google Cloud APIs are only consumed via VPC Service Controls.

What should you do?

A. 1. Set up a Cloud VPN link between the on-premises environment and Google Cloud.

2. Configure private access using the restricted googleapis.com domains in on-premises DNS configurations.

B. 1. Set up a Partner Interconnect link between the on-premises environment and Google Cloud.

2. Configure private access using the private.googleapis.com domains in on-premises DNS configurations.

C. 1. Set up a Direct Peering link between the on-premises environment and Google Cloud.

2. Configure private access for both VPC subnets.

D. 1. Set up a Dedicated Interconnect link between the on-premises environment and Google Cloud.

2. Configure private access using the restricted.googleapis.com domains in on-premises DNS configurations.

Correct Answer: D

restricted.googleapis.com (199.36.153.4/30) only provides access to Cloud and Developer APIs that support VPC Service Controls. VPC Service Controls are enforced for these services https://cloud.google.com/vpc/docs/configure-privategoogle-access-hybrid

QUESTION 12

An organization is moving applications to Google Cloud while maintaining a few mission-critical applications on-premises. The organization must transfer the data at a bandwidth of at least 50 Gbps. What should they use to ensure secure continued connectivity between sites?

A. Dedicated Interconnect

B. Cloud Router

C. Cloud VPN

D. Partner Interconnect

Correct Answer: A

Reference: https://cloud.google.com/architecture/migration-to-google-cloud-transferring-your-large- datasets https://cloud.google.com/network-connectivity/docs/interconnect/concepts/overview

QUESTION 13

You are tasked with exporting and auditing security logs for login activity events for Google Cloud console and API calls that modify configurations to Google Cloud resources. Your export must meet the following requirements:

Export related logs for all projects in the Google Cloud organization.

Export logs in near real-time to an external SIEM.

What should you do? (Choose two.)

A. Create a Log Sink at the organization level with a Pub/Sub destination.

B. Create a Log Sink at the organization level with the includeChildren parameter, and set the destination to a Pub/Sub topic.

C. Enable Data Access audit logs at the organization level to apply to all projects.

D. Enable Google Workspace audit logs to be shared with Google Cloud in the Admin Console.

E. Ensure that the SIEM processes the AuthenticationInfo field in the audit log entry to gather identity information.

Correct Answer: BD

Reference:

https://www.datadoghq.com/blog/monitoring-gcp-audit-logs/ https://cloud.google.com/logging/docs/audit/gsuite-audit-logging#services "Google Workspace Login Audit: Login Audit logs track user sign-ins to your domain. These logs only

record the login event. They don\\'t record which system was used to perform the login action."

QUESTION 14

You are in charge of migrating a legacy application from your company datacenters to GCP before the current maintenance contract expires. You do not know what ports the application is using and no documentation is available for you to check. You want to complete the migration without putting your environment at risk.

What should you do?

A. Migrate the application into an isolated project using a "Lift and Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

B. Migrate the application into an isolated project using a "Lift and Shift" approach in a custom network. Disable all traffic within the VPC and look at the Firewall logs to determine what traffic should be allowed for the application to work properly.

C. Refactor the application into a micro-services architecture in a GKE cluster. Disable all traffic from outside the cluster using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

D. Refactor the application into a micro-services architecture hosted in Cloud Functions in an isolated project. Disable all traffic from outside your project using Firewall Rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

Correct Answer: A

Migrate the application into an isolated project using a "Lift and Shift" approach. Enable all internal TCP traffic using VPC Firewall rules. Use VPC Flow logs to determine what traffic should be allowed for the application to work properly.

QUESTION 15

You plan to use a Google Cloud Armor policy to prevent common attacks such as cross-site scripting (XSS) and SQL injection (SQLi) from reaching your web application\\'s backend. What are two requirements for using Google Cloud Armor security policies? (Choose two.)

A. The load balancer must be an external SSL proxy load balancer.

B. Google Cloud Armor Policy rules can only match on Layer 7 (L7) attributes.

C. The load balancer must use the Premium Network Service Tier.

D. The backend service\\'s load balancing scheme must be EXTERNAL.

E. The load balancer must be an external HTTP(S) load balancer.

Correct Answer: DE

https://cloud.google.com/armor/docs/security-policy-overview#requirements says: The backend service\\'s load balancing scheme must be EXTERNAL, or EXTERNAL_MANAGED *** if you are using global external HTTP(S) load balancer ***.