Vendor: Google

Exam Code: Professional-Cloud-Security-Engineer

Exam Name: Professional Cloud Security Engineer

Version: DEMO

QUESTION 1
Your company requires the security and network engineering teams to identify all network anomalies and be able to capture payloads within VPCs. Which method should you use?

A. Define an organization policy constraint.
B. Configure packet mirroring policies.
C. Enable VPC Flow Logs on the subnet.
D. Monitor and analyze Cloud Audit Logs.

Answer: B
Explanation:
https://cloud.google.com/vpc/docs/packet-mirroring
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

QUESTION 2
You need to enforce a security policy in your Google Cloud organization that prevents users from exposing objects in their buckets externally. There are currently no buckets in your organization. Which solution should you implement proactively to achieve this goal with the least operational overhead?

A. Create an hourly cron job to run a Cloud Function that finds public buckets and makes them private.
B. Enable the constraints/storage.publicAccessPrevention constraint at the organization level.
C. Enable the constraints/storage.uniformBucketLevelAccess constraint at the organization level.
D. Create a VPC Service Controls perimeter that protects the storage.googleapis.com service in your projects that contains buckets. Add any new project that contains a bucket to the perimeter.

Answer: B
Explanation:
https://cloud.google.com/storage/docs/public-access-prevention
Public access prevention protects Cloud Storage buckets and objects from being accidentally exposed to the public.
If your bucket is contained within an organization, you can enforce public access prevention by using the organization policy constraint storage.publicAccessPrevention at the project, folder, or organization level.

QUESTION 3
You are consulting with a client that requires end-to-end encryption of application data (including data in transit, data in use, and data at rest) within Google Cloud.
Which options should you utilize to accomplish this? (Choose two.)

A. External Key Manager
B. Customer-supplied encryption keys
C. Hardware Security Module
D. Confidential Computing and Istio
E. Client-side encryption

Answer: DE
Explanation:

Google Cloud customers with additional requirements for encryption of data over WAN can choose to implement further protections for data as it moves from a user to an application, or virtual machine to virtual machine. These protections include IPSec tunnels, Gmail S/MIME, managed SSL certificates, and Istio.
https://cloud.google.com/docs/security/encryption-in-transit

QUESTION 4
You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your VPCs based on network logs. However, you want to explore your environment using network payloads and headers. Which Google Cloud product should you use?

A. Cloud IDS
B. VPC Service Controls logs
C. VPC Flow Logs
D. Google Cloud Armor
E. Packet Mirroring

Answer: E
Explanation:
https://cloud.google.com/vpc/docs/packet-mirroring
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

QUESTION 5
You are working with a client who plans to migrate their data to Google Cloud. You are responsible for recommending an encryption service to manage their encrypted keys. You have the following requirements:

- The master key must be rotated at least once every 45 days.
- The solution that stores the master key must be FIPS 140-2 Level 3 validated.
- The master key must be stored in multiple regions within the US for redundancy.

Which solution meets these requirements?

A. Customer-managed encryption keys with Cloud Key Management Service
B. Customer-managed encryption keys with Cloud HSM
C. Customer-supplied encryption keys
D. Google-managed encryption keys

Answer: B
Explanation:
https://cloud.google.com/docs/security/key-management-deep-dive
https://cloud.google.com/kms/docs/faq
"Keys generated with protection level HSM, and the cryptographic operations performed with them, comply with FIPS 140-2 Level 3."

QUESTION 6
You have created an OS image that is hardened per your organization's security standards and is being stored in a project managed by the security team. As a Google Cloud administrator, you

need to make sure all VMs in your Google Cloud organization can only use that specific OS image while minimizing operational overhead. What should you do? (Choose two.)

A. Grant users the compute.imageUser role in their own projects.
B. Grant users the compute.imageUser role in the OS image project.
C. Store the image in every project that is spun up in your organization.
D. Set up an image access organization policy constraint, and list the security team managed project in the project's allow list.
E. Remove VM instance creation permission from users of the projects, and only allow you and your team to create VM instances.

Answer: BD
Explanation:
https://cloud.google.com/resource-manager/docs/organization-policy/org-policy-constraints
- constraints/compute.trustedImageProjects
This list constraint defines the set of projects that can be used for image storage and disk instantiation for Compute Engine.
If this constraint is active, only images from trusted projects will be allowed as the source for boot disks for new instances.

QUESTION 7
Your security team wants to implement a defense-in-depth approach to protect sensitive data stored in a Cloud Storage bucket. Your team has the following requirements:

- The Cloud Storage bucket in Project A can only be readable from Project B.
- The Cloud Storage bucket in Project A cannot be accessed from outside the network.
- Data in the Cloud Storage bucket cannot be copied to an external Cloud Storage bucket.

What should the security team do?

A. Enable domain restricted sharing in an organization policy, and enable uniform bucket-level access on the Cloud Storage bucket.
B. Enable VPC Service Controls, create a perimeter around Projects A and B, and include the Cloud Storage API in the Service Perimeter configuration.
C. Enable Private Access in both Project A and B's networks with strict firewall rules that allow communication between the networks.
D. Enable VPC Peering between Project A and B's networks with strict firewall rules that allow communication between the networks.

Answer: B
Explanation:
VPC Peering is between organizations not between Projects in an organization. That is Shared VPC. In this case, both projects are in same organization so having VPC Service Controls around both projects with necessary rules should be fine.
https://cloud.google.com/vpc-service-controls/docs/overview

QUESTION 8
You have been tasked with inspecting IP packet data for invalid or malicious content. What should you do?

A. Use Packet Mirroring to mirror traffic to and from particular VM instances. Perform inspection using security software that analyzes the mirrored traffic.

B. Enable VPC Flow Logs for all subnets in the VPC. Perform inspection on the Flow Logs data using Cloud Logging.
C. Configure the Fluentd agent on each VM Instance within the VPC. Perform inspection on the log data using Cloud Logging.
D. Configure Google Cloud Armor access logs to perform inspection on the log data.

Answer: A
Explanation:
https://cloud.google.com/vpc/docs/packet-mirroring
Packet Mirroring clones the traffic of specified instances in your Virtual Private Cloud (VPC) network and forwards it for examination. Packet Mirroring captures all traffic and packet data, including payloads and headers.

QUESTION 9
You are a security administrator at your company and are responsible for managing access controls (identification, authentication, and authorization) on Google Cloud. Which Google-recommended best practices should you follow when configuring authentication and authorization? (Choose two.)

A. Use Google default encryption.
B. Manually add users to Google Cloud.
C. Provision users with basic roles using Google's Identity and Access Management (IAM) service.
D. Use SSO/SAML integration with Cloud Identity for user authentication and user lifecycle management.
E. Provide granular access with predefined roles.

Answer: DE
Explanation:
https://cloud.google.com/iam/docs/using-iam-securely#least_privilege
Basic roles include thousands of permissions across all Google Cloud services. In production environments, do not grant basic roles unless there is no alternative. Instead, grant the most limited predefined roles or custom roles that meet your needs.

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

Answer: B
Explanation:
https://cloud.google.com/kms/docs/using-other-products#cmek_integrations
CMEK is supported for all the listed google services.

QUESTION 11

Which Identity-Aware Proxy role should you grant to an Identity and Access Management (IAM) user to access HTTPS resources?

A. Security Reviewer
B. IAP-Secured Tunnel User
C. IAP-Secured Web App User
D. Service Broker Operator

Answer: C
Explanation:
https://cloud.google.com/iap/docs/managing-access
"IAP-Secured Web App User: Grants access to the app and other HTTPS resources that use IAP."

QUESTION 12
You need to audit the network segmentation for your Google Cloud footprint. You currently operate Production and Non-Production infrastructure-as-a-service (IaaS) environments. All your VM instances are deployed without any service account customization.
After observing the traffic in your custom network, you notice that all instances can communicate freely `" despite tag-based VPC firewall rules in place to segment traffic properly `" with a priority of 1000. What are the most likely reasons for this behavior?

A. All VM instances are missing the respective network tags.
B. All VM instances are residing in the same network subnet.
C. All VM instances are configured with the same network route.
D. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 999.
E. A VPC firewall rule is allowing traffic between source/targets based on the same service account with priority 1001.

Answer: D
Explanation:
priority 999 is a higher priority than 1000, so if 999 has allow all policy then any deny policy with lower priority will not be applied.

QUESTION 13
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 IAM 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.

Answer: A

Explanation:
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 14
You are in charge of creating a new Google Cloud organization for your company. Which two actions should you take when creating the super administrator accounts? (Choose two.)

A. Create an access level in the Google Admin console to prevent super admin from logging in to Google Cloud.
B. Disable any Identity and Access Management (IAM) roles for super admin at the organization level in the Google Cloud Console.
C. Use a physical token to secure the super admin credentials with multi-factor authentication (MFA).
D. Use a private connection to create the super admin accounts to avoid sending your credentials over the Internet.
E. Provide non-privileged identities to the super admin users for their day-to-day activities.

Answer: CE
Explanation:
https://cloud.google.com/resource-manager/docs/super-admin-best-practices#discourage_super_admin_account_usage
- Use a security key or other physical authentication device to enforce two-step verification
- Give super admins a separate account that requires a separate login

QUESTION 15
Your company's cloud security policy dictates that VM instances should not have an external IP address. You need to identify the Google Cloud service that will allow VM instances without external IP addresses to connect to the internet to update the VMs. Which service should you use?

A. Identity Aware-Proxy
B. Cloud NAT
C. TCP/UDP Load Balancing
D. Cloud DNS

Answer: B
Explanation:
https://cloud.google.com/nat/docs/overview
"Cloud NAT (network address translation) lets certain resources without external IP addresses create outbound connections to the internet."

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**