1. Your team needs to make sure that a Compute Engine instance does not have access to the

internet or to any Google APIs or services. Which two settings must remain disabled to meet these requirements? (Choose two.)

* Public IP and Private Google Access

1. Which two implied firewall rules are defined on a VPC network? (Choose two.)

|  |
| --- |
| * A rule that allows all outbound connections * A rule that denies all inbound connections |

1. A customer needs an alternative to storing their plain text secrets in their source-code

management (SCM) system. How should the customer achieve this using Google Cloud Platform?

|  |
| --- |
| * Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage. |

1. 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?

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

1. When creating a secure container image, which two items should you incorporate into the build if possible? (Choose two.)

* Package a single app as a container.
* Remove any unnecessary tools not needed by the app.

1. 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?

|  |
| --- |
| * Cloud Armor |

1. A company is running workloads in a dedicated server room. They must only be accessed from within the private company network. You need to connect to these workloads from Compute Engine instances within a Google Cloud Platform project.

Which two approaches can you take to meet the requirements? (Choose two.)

* Configure the project with Cloud VPN
* Configure the project with Cloud Interconnect

1. A customer implements Cloud Identity-Aware Proxy for their ERP system hosted on

Compute Engine. Their security team wants to add a security layer so that ERP systems only accept traffic from Cloud Identity-Aware Proxy. What should the customer do to meet these requirements?

* Make sure that the ERP system can validate the JWT assertion in the HTTP requests.

1. A company has been running their application on Compute Engine. A bug in the application allowed a malicious user to repeatedly execute a script that results in the Compute Engine instance crashing. Although the bug has been fixed, you want to get notified in case this hack re-occurs. What should you do?

* Create an Alerting Policy in Stackdriver using a Process Health condition,checking that the no. of executions of the script remains below the desired threshold.Enable notificatio

1. Your team needs to obtain a unified log view of all development cloud projects in your SIEM. The development projects are under the NONPROD organization folder with the test and pre-production projects. The development projects share the ABC-BILLING billing account with the rest of the organization.

Which logging export strategy should you use to meet the requirements?

* Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project.
* Subscribe SIEM to the topic.

1. 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?

* DNS Security Extensions

1. A customer deploys an application to App Engine and needs to check for Open Web

Application Security Project (OWASP) vulnerabilities. Which service should be used to accomplish this?

* Web Security Scanner

1. A customer's data science group wants to use (GCP) for their analytics workloads. Company policy dictates that all data must be company-owned and all user authentications must go through their own Security Assertion Markup Language (SAML) 2.0 Identity Provider (IdP). Infrastructure Operations Systems Engineer was trying to set up Cloud Identity for the customer & realized that their domain was already being used by G Suite. How should you best advise the Systems Engineer to proceed with the least disruption?

* Ask customer's management to discover any other uses of Google managed services, and work with the existing Super Administrator.

1. A business unit at a multinational corporation signs up for GCP and starts moving workloads into GCP. The business unit creates a Cloud Identity domain with an organizational resource that has hundreds of projects. Your team becomes aware of this and wants to take over managing permissions and auditing the domain resources.

Which type of access should your team grant to meet this requirement?

* Organizational Role Administrator

1. An application running on a Compute Engine instance needs to read data from a Cloud

Storage bucket. Your team doesn’t allow Cloud Storage buckets to be globally readable & wants to ensure the principle of least privilege. Which option meets the requirement of your team?

* Use a service account with read-only access to the Cloud Storage bucket to retrieve the credentials from the instance metadata

1. An organization's typical network and security review consists of analyzing application transit routes, request handling, and firewall rules. They want to enable their developer teams to deploy new applications without the overhead of this full review. How should you advise this organization?

* Mandate use of infra as code & provide static analysis in the CI/CD pipelines to enforce policies.

1. An employer wants to track how bonus compensations have changed over time to identify employee outliers and correct earning disparities. This task must be performed without exposing the sensitive compensation data for any individual and must be reversible to identify the outlier. Which Cloud Data Loss Prevention API technique should you use to accomplish this?

* CryptoReplaceFfxFpeConfig

1. An organization adopts Google Cloud Platform (GCP) for application hosting services and needs guidance on setting up password requirements for their Cloud Identity account. The organization has a password policy requirement that corporate employee passwords must have a minimum number of characters.

Which Cloud Identity password guidelines can the organization use to inform their new requirements?

* Set the minimum length for passwords to be 8 characters.

1. You need to follow Google-recommended practices to leverage envelope encryption and encrypt data at the application layer. What should you do?

* Generate a data encryption key (DEK) locally to encrypt the data, and generate a new key encryption key (KEK) in Cloud KMS to encrypt the DEK. Store both the encrypted data and the encrypted DEK.

1. How should a customer reliably deliver Stackdriver logs from GCP to their on-premises

SIEM system?

* Configure Organizational Log Sinks to export logs to a Cloud Pub/Sub Topic, which will be sent to the SIEM via Dataflow.

1. In order to meet PCI DSS requirements, a customer wants to ensure that all outbound traffic is authorized. Which two cloud offerings meet this requirement without additional compensating controls? (Choose two.)

* Compute Engine
* Google Kubernetes Engine

1. A website design company recently migrated all customer sites to App Engine. Some sites are still in progress and should only be visible to customers and company employees from any location. Which solution will restrict access to the in-progress sites?

* Enable Cloud Identity-Aware Proxy (IAP), and allow access to a Google Group that contains the customer and employee user accounts.

1. When working with agents in the support center via online chat, your organization's

customers often share pictures of their documents with personally identifiable information (PII). Your leadership team is concerned that this PII is being stored as part of the regular chat logs, which are reviewed by internal or external analysts for customer service trends. You want to resolve this concern while still maintaining data utility. What should you do?

* Use the image inspection and redaction actions of the DLP API to redact PII from the images before storing them for analysis.

1. A company's application is deployed with a user-managed Service Account key. U want to use Google-recommended practices to rotate the key. What should U do?

* Create a new key, and use the new key in the application. Delete the old key from the Service Account

1. Your team needs to configure their Google Cloud Platform (GCP) environment so they can centralize the control over networking resources like firewall rules, subnets, and routes. They also have an on-premises environment where resources need access back to the GCP resources through a private VPN connection. The networking resources will need to be controlled by the network security team. Which type of networking design shld your team use to meet these requirements?

* Shared VPC Network with a host project and service projects

1. An organization is migrating from their current on-premises productivity software systems to G Suite. Some network security controls were in place that were mandated by a regulatory body in their region for their previous on-premises system. The organization's risk team wants to ensure that network security controls are maintained and effective in G Suite. A security architect supporting this migration has been asked to ensure that network security controls are in place as part of the new shared responsibility model between the organization and Google Cloud.

What solution would help meet the requirements?

* Network security is a built-in solution and Google's Cloud responsibility for SaaS products like G Suite

1. A customer's company has multiple business units. Each business unit operates

independently, and each has their own engineering group. Your team wants visibility into all projects created within the company and wants to organize their Google Cloud Platform (GCP) projects based on different business units. Each business unit also requires separate sets of IAM permissions. Which strategy should you use to meet these needs?

|  |
| --- |
| * A. Create an organization node, and assign folders for each business unit. |

1. A company has redundant mail servers in different Google Cloud Platform regions and wants

to route customers to the nearest mail server based on location. How should the company accomplish this?

* Configure TCP Proxy Load Balancing as a global load balancing service listening on port 995.

1. Your team sets up a Shared VPC Network where project co-vpc-prod is the host project. Your team has configured the firewall rules, subnets, and VPN gateway on the host project. They need to enable Engineering Group A to attach a Compute Engine instance to only the 10.1.1.0/24 subnet. What should your team grant to Engineering Group A to meet this requirement?

* Compute Network User Role at the subnet level.

1. A company migrated their entire data/center to Google Cloud Platform. It is running thousands of instances across multiple projects managed by different departments. You want to have a historical record of what was running in Google Cloud Platform at any point in time. What should you do?

* Use Forseti Security to automate inventory snapshots.

1. An organization is starting to move its infrastructure from its on-premises environment to

(GCP). The first step the organization wants to take is to migrate its current data backup and disaster recovery solutions to GCP for later analysis. The organization's production environment will remain on- premises for an indefinite time. The organization wants a scalable and cost-efficient solution. Which GCP solution should the organization use?

* Cloud Storage using a scheduled task and gsutil

1. You are creating an internal App Engine application that needs to access a user's Google

Drive on the user's behalf. Your company does not want to rely on the current user's credentials. It also wants to follow Google-recommended practices. What should you do?

* Create a new service account, and grant it G Suite domain-wide delegation. Have the application use it to impersonate the user.

1. A customer wants to move their sensitive workloads to a Compute Engine-based cluster using Managed Instance Groups (MIGs). The jobs are bursty and must be completed quickly. They have a requirement to be able to control the key lifecycle. Which boot disk encryption solution should you use on the cluster to meet this customer's requirements?

* Use Forseti Security to automate inventory snapshots.

1. 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?

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

1. You are a member of the security team at an organization. Your team has a single GCP project with credit card payment processing systems alongside web applications and data processing systems. You want to reduce the scope of systems subject to PCI audit standards. What should you do?

* Move the cardholder data environment into a separate GCP project

1. A retail customer allows users to upload comments and product reviews. The customer needs to make sure the text does not include sensitive data before the comments or reviews are published. Which Google Cloud Service should be used to achieve this?

* Cloud Data Loss Prevention API

1. A company allows every emp to use Google Cloud Platform. Each department has a

Google Group, with all department members as group members. If a department member creates a new project, all members of that dept should automatically have read-only access to all new project resources. Members of any other department should not have access to the project. U need to configure this behavior. What should you do to meet these req?

* Create a Folder per department under the Organization. For each department's Folder, assign the Project Viewer role to the Google Group related to that department.

1. 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?

* Use the gsutil command line tool to upload the object to Cloud Storage, and specify

1. A customer has 300 engineers. The company wants to grant different levels of access and

efficiently manage IAM permissions between users in the development and production environment projects. Which two steps should the company take to meet these req? (two)

* Create a folder for each development and production environment.
* Create a Google Group for the Engineering team, and assign permissions at the folder level.

1. You want to evaluate your organization's Google Cloud instance for PCI compliance. You need to identify Google's inherent controls. Which document should you review to find the info?

* Google Cloud Platform: Customer Responsibility Matrix

1. Your company runs a website that will store PII on Google Cloud Platform. To comply with data privacy regulations, this data can only be stored for a specific amount of time and must be fully deleted after this specific period. Data that has not yet reached the time period should not be deleted. You want to automate the process of complying with this regulation.

What should you do?

* Store the data in a single Cloud Storage bucket and configure the bucket's Time to Live.

1. A DevOps team will create a new container to run on Google Kubernetes Engine. As the application will be internet-facing, they want to minimize the attack surface of the container. What should they do?

* Build small containers using small base images.

1. While migrating your organization's infrastructure to GCP, a large number of users will need to access GCP Console. The Identity Management team already has a well-established way to manage your users and want to keep using your existing Active Directory or LDAP server along with the existing SSO password. What should you do?

* Use Google Cloud Directory Sync to synchronize the data in Google domain with your existing Active Directory or LDAP server

1. Your company is using GSuite & has developed an application meant for internal usage on Google App Engine. U need to make sure that an external user can’t gain access to the application even when an employee's password has been compromised.What should u do?

* Enforce 2-factor authentication in GSuite for all users.

1. A large financial institution is moving its Big Data analytics to Google Cloud Platform. They want to have maximum control over the encryption process of data stored at rest in BigQuery. What technique should the institution use?

* Customer-managed encryption keys (CMEK)

1. A company is deploying their application on Google Cloud Platform. Company policy

requires long-term data to be stored using a solution that can automatically replicate data over at least two geographic places. Which Storage solution are they allowed to use?

* Cloud BigQuery

1. A large e-retailer is moving to Google Cloud Platform with its ecommerce website. The company wants to ensure payment information is encrypted between the customer's browser and GCP when the customers checkout online. What should they do?

* Configure an SSL Certificate on an L7 Load Balancer and require encryption

1. Applications often require access to `secrets` - small pieces of sensitive data at build or run

time. The administrator managing these secrets on GCP wants to keep a track of `who did what, where, and when?` within their GCP projects. Which two log streams would provide the information that the administrator is looking for? (Choose two.)

* Admin Activity logs
* Data Access Logs

1. 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?

* Migrate the application into an isolated project using a ג€Lift & Shiftג€ 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.

1. Your company has deployed an application on Compute Engine. The application is accessible by clients on port 587. You need to balance the load between the different instances running the application. The connection should be secured using TLS, and terminated by the Load Balancer. What type of Load Balancing should you use?

SSL Proxy Load Balancing

1. You want to limit the images that can be used as the source for boot disks. These images will be stored in a dedicated project.What should be done ?

* Use the Organization Policy Service to create a compute.trustedimageProjects constraint on the organization level. List the trusted project as the whitelist in an allow operation.

1. Your team needs to prevent users from creating projects in the organization. Only the

DevOps team should be allowed to create projects on behalf of the requester. Which two tasks should your team perform to handle this request? (Choose two.)

* Remove all users from the Project Creator role at the organizational level.
* Add a designated group of users to the Project Creator role at the organizational level

1. A customer deployed an application on Compute Engine that takes advantage of the elastic nature of cloud computing. How can you work with Infrastructure Operations Engineers to best ensure tht Windows Compute Engine VMs are up to date with all the latest OS patches?

* Build new base images when patches are available, and use a CI/CD pipeline to rebuild VMs, deploying incrementally.

1. Your team needs to make sure that their backend database can only be accessed by the frontend application & no other instances on the n/w. How should your team design this n/w?

* Create an ingress firewall rule to allow access only from the application to the db using firewall tags.

1. An organization receives an increasing number of phishing emails. Which method should be used to protect employee credentials in this situation?

* Multifactor Authentication

1. A customer is collaborating with another company to build an application on Compute Engine. The customer is building the application tier in their GCP Organization, and the other company is building the storage tier in a different GCP Organization. This is a 3-tier web application. Communication between portions of the application must not traverse the public internet by any means. Which connectivity option should be implemented?

* VPC peering

1. Your team wants to make sure Compute Engine instances running in your production project don’t have public IP addresses. The frontend application Compute Engine instances will require public IPs. The product engineers have the Editor role to modify resources. Your team wants to enforce this req. How should your team meet these req.?

* Set up an organization policy to only permit public IPs for the front-end Compute Engine instances.

1. Which two security characteristics are related to the use of VPC peering to connect two VPC

networks? (Choose two.)

* Non-transitive peered networks; where only directly peered networks can communicate
* Ability to peer networks that belong to different Google Cloud organizations

1. A patch for a vulnerability has been released, and a DevOps team needs to update their running containers in Google Kubernetes Engine (GKE). How should the DevOps team accomplish this?

* Update the application code or apply a patch, build a new image, and redeploy it

1. A company is running their webshop on Google Kubernetes Engine and wants to analyze

customer transactions in BigQuery. You need to ensure that no credit card numbers are stored in BigQuery. What should you do?

* Use the Cloud Data Loss Prevention API to redact related infoTypes before data is ingested into BigQuery.

1. A customer wants to deploy a large number of 3-tier web applications on Compute Engine. How should the customer ensure authenticated network separation between the different tiers of the application?

* Run each tier with a different Service Account (SA), and use SA-based firewall rules.

1. A manager wants to start retaining security event logs for 2 years while minimizing costs. You write a filter to select the appropriate log entries. Where should you export the logs?

* Cloud Storage bucket

1. For compliance reasons, an organization needs to ensure that in-scope PCI Kubernetes Pods

reside on `in-scope` Nodes only. These Nodes can only contain the `in-scope` Pods. How should the organization achieve this objective?

* Add a nodeSelector field to the pod configuration to only use the Nodes labeled inscope: true.

1. In an effort for your company messaging app to comply with FIPS 140-2, a decision was made to use GCP compute and network services. The messaging app architecture includes a Managed Instance Group (MIG) that controls a cluster of Compute Engine instances. The instances use Local SSDs for data caching and UDP for instance-to-instance communications. The app development team is willing to make any changes necessary to comply with the standard

Which options should you recommend to meet the requirements?

* Encrypt all cache storage and VM-to-VM communication using the BoringCrypto module.

1. A customer has an analytics workload running on Compute Engine that should have limited internet access. Your team created an egress firewall rule to deny (priority 1000) all traffic to the internet. The Compute Engine instances now need to reach out to the public repository to get security updates. What should your team do?

* Create an egress firewall rule to allow traffic to the CIDR range of the repository with a priority less than 1000.

1. You want data on Compute Engine disks to be encrypted at rest with keys managed by Cloud Key Management Service (KMS). Cloud Identity and Access Management (IAM) permissions to these keys must be managed in a grouped way because the permissions should be the same for all keys. What should you do?

* Create a single KeyRing for all persistent disks and all Keys in this KeyRing. Manage the IAM permissions at the KeyRing level.

1. A company is backing up application logs to a Cloud Storage bucket shared with both

analysts and the administrator. Analysts should only have access to logs that do not contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible by the administrator. What should you do?

* Use Cloud Pub/Sub and Cloud Functions to trigger a Data Loss Prevention scan every time a file is uploaded to the shared bucket. If the scan detects PII, have the function move into a Cloud Storage bucket only accessible by the administrator.

1. A customer terminates an engineer and needs to make sure the engineer's Google account is automatically deprovisioned. What should the customer do?

* Configure Cloud Directory Sync with their directory service to provision and deprovision users from Cloud Identity

1. An organization is evaluating the use of Google Cloud Platform (GCP) for certain IT workloads. A well-established directory service is used to manage user identities and

lifecycle management. This directory service must continue for the organization to use as the

`source of truth` directory for identities.

Which solution meets the organization's requirements?

* Google Cloud Directory Sync (GCDS)

1. Which international compliance standard provides guidelines for information security

controls applicable to the provision and use of cloud services?

* ISO 27017

1. You will create a new Service Account that should be able to list the Compute Engine

instances in the project. You want to follow Google-recommended practices. What should you do?

* Create a custom role with the permission compute.instances.list and grant the Service Account this role.

1. In a shared security responsibility model for IaaS, which two layers of the stack does the customer share responsibility for? (Choose two.)

* Network Security and Access Policy

1. An organization is starting to move its infrastructure from its on-premises environment to Google Cloud Platform (GCP). The first step the organization wants to take is to migrate its ongoing data backup and disaster recovery solutions to GCP. The organization's on-premises production environment is going to be the next phase for migration to GCP. Stable networking connectivity between the on-premises environment and GCP is also being implemented.

Which GCP solution should the organization use?

* Cloud Storage using a scheduled task and gsutil via Cloud Interconnect

1. What are the steps to encrypt data using envelope encryption

✑ Generate a data encryption key (DEK) locally.

✑ Encrypt data with the DEK.

✑ Use a key encryption key (KEK) to wrap the DEK.

.

✑ Store the encrypted data and the wrapped DEK

1. A customer wants to make it convenient for their mobile workforce to access a CRM web

interface that is hosted on GCP. The CRM can only be accessed by someone on the corporate network. The customer wants to make it available over the internet. Your team requires an authentication layer in front of the application that supports two-factor authentication. Which GCP product should the customer implement to meet these req.?

* Cloud Identity-Aware Proxy

1. Your company is storing sensitive data in Cloud Storage. You want a key generated on

premises to be used in the encryption process. What should be done ?

**Most Voted**

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

1. Last week, a company deployed a new App Engine application that writes logs to BigQuery. No other workloads are running in the project. You need to validate that all data written the BigQuery was done using the App Engine Default Service Account. What should you do?

* Use Cloud Logging and filter on BigQuery Insert Jobs. 2. Click on the email address in line with the App Engine Default Service Account in the authentication field. 3. Click Hide Matching Entries. 4. Make sure the resulting list is empty.

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

* Organization Administrator and Super Admin

1. An organization's security and risk management teams are concerned about where their

responsibility lies for certain production workloads they are running in Google Cloud and where Google's responsibility lies. They are mostly running workloads using Google Cloud's platform-as-a-Service (PaaS) offerings, including App Engine primarily. Which area in the technology stack should they focus on as their primary responsibility when using App Engine?

* Defending against XSS and SQLi attacks

1. 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?

* Cloud Armour

1. A customer is running an analytics workload on Google Cloud Platform where Compute Engine instances are accessing data stored on Cloud Storage. Your team wants to make sure that this workload will not be able to access, or be accessed from, the internet. Which two strategies should your team use to meet these requirements? (Choose two.)

* Configure Private Google Access on the Compute Engine subnet
* Avoid assigning public IP addresses to the Compute Engine cluster

1. A customer wants to run a batch processing system on VMs and store the output files in a

Cloud Storage bucket. The networking and security teams have decided that no VMs may reach the public internet. How should this be accomplished?

* Enable Private Google Access.

1. As adoption of the Cloud Data Loss Prevention (Cloud DLP) API grows within your company, you need to optimize usage to reduce cost. Cloud DLP target data is stored in Cloud Storage and BigQuery. The location and region are identified as a suffix in the resource name. Which cost reduction options should you recommend?

* Use rowsLimit and bytesLimitPerFile to sample data and use CloudStorageRegexFileSet to limit scans.

1. Your team uses a service account to authenticate data transfers from a given Compute Engine

virtual machine instance of to a specified Cloud Storage bucket. An engineer accidentally deletes the service account, which breaks application functionality. You want to recover the application as quickly as possible without compromising security. What should you do?

* Use the undelete command to recover the deleted service account.

1. You are the Security Admin in your company. You want to synchronize all security groups that have an email address from your LDAP directory in Cloud IAM. What should you do?

* Configure Google Cloud Directory Sync to sync security groups using LDAP search rules that have ג€user email addressג€ as the attribute to facilitate one-way sync.

1. You are part of a security team investigating a compromised service account key. You need to audit which new resources were created by the service account.

What should you do?

* Query Admin Activity logs.

1. You have an application where the frontend is deployed on a managed instance group in

subnet A and the data layer is stored on a mysql Compute Engine virtual machine (VM) in subnet B on the same VPC. Subnet A and Subnet B hold several other Compute Engine VMs. You only want to allow the application frontend to access the data in the application's mysql instance on port 3306. What should you do?

* Configure an ingress firewall rule that allows communication from the frontend's unique service account to the unique service account of the mysql Compute Engine VM on port 3306

1. Your company operates an application instance group that is currently deployed behind a Google Cloud load balancer in us-central-1 and is configured to use the Standard Tier network. The infrastructure team wants to expand to a second Google Cloud region, us-east-2. You need to set up a single external IP address to distribute new requests to the instance groups in both regions. What should you do?

* Change the load balancer frontend configuration to use the Premium Tier network, and add the new instance group.

1. You are the security admin of your company. You have 3,000 objects in your Cloud Storage bucket. You do not want to manage access to each object individually. You also do not want the uploader of an object to always have full control of the object. However, you want to use Cloud Audit Logs to manage access to your bucket. What should you do?

* Set up Uniform bucket-level access on the Cloud Storage bucket and manage access for users using IAM.

1. You are the security admin of your company. Your development team creates multiple GCP projects under the "implementation" folder for several dev, staging, and production workloads. You want to prevent data exfiltration by malicious insiders or compromised code by setting up a security perimeter. However, you do not want to restrict communication between the projects. What should you do?

* Use an infrastructure-as-code s/w tool to set up a single service perimeter and to deploy a Cloud Function that monitors the "implementation" folder via Stackdriver and Cloud Pub/Sub. When the function notices that a new project is added to the folder, it executes Terraform to add the new project to the associated perimeter.

1. You need to provide a corporate user account in Google Cloud for each of your developers and operational staff who need direct access to GCP resources. Corporate policy requires you to maintain the user identity in a third-party identity management provider and leverage single sign-on. You learn that a significant number of users are using their corporate domain email addresses for personal Google accounts, and you need to follow Google recommended practices to convert existing unmanaged users to managed accounts.

Which two actions should you take? (Choose two.)

* Use Google Cloud Directory Sync to synchronize your local identity management system to Cloud Identity.
* Use the Transfer Tool for Unmanaged Users (TTUU) to find users with conflicting accounts and ask them to transfer their personal Google accounts.

1. You are on your company's development team. You noticed that your web application hosted in staging on GKE dynamically includes user data in web pages without first properly validating the inputted data. This could allow an attacker to execute gibberish commands and display arbitrary content in a victim user's browser in a production environment. How should you prevent and fix this vulnerability?

* Use Web Security Scanner in staging to simulate an XSS injection attack, and then use a templating system that supports contextual auto-escaping

1. You are part of a security team that wants to ensure that a Cloud Storage bucket in Project A can only be readable from Project B. You also want to ensure that data in the Cloud Storage bucket cannot be accessed from or copied to Cloud Storage buckets outside the network, even if the user has the correct credentials. What should you do?

* Enable VPC Service Controls, create a perimeter with Project A and B, and include Cloud Storage service.

1. You are responsible for protecting highly sensitive data in BigQuery. Your operations teams need access to this data, but given privacy regulations, you want to ensure that they cannot read the sensitive fields such as email addresses and first names. These specific sensitive fields should only be available on a need-to- know basis to the HR team. What should you do?

* Perform tokenization for Pseudonymization with the DLP API and store that data in BigQuery for later use.

1. You are a Security Administrator at your organization. You need to restrict service account creation capability within production environments. You want to accomplish this centrally across the orz

* Use organization policy constraints/iam.disableServiceAccountCreation boolean to disable the creation of new service accounts

1. You are the project owner for a regulated workload that runs in a project you own and manage as an Identity and Access Management (IAM) admin. For an upcoming audit, you need to provide access reviews evidence. Which tool should you use?

* Policy Analyzer

1. Your organization has implemented synchronization and SAML federation between Cloud Identity and Microsoft Active Directory. You want to reduce the risk of Google Cloud user accounts being compromised. What should you do?

* Create an Active Directory domain password policy with strong password settings, and configure post-SSO (single sign-on) 2-Step Verification with security keys in the Google Admin console.

1. You have been tasked with implementing external web application protection against common web application attacks for a public application on Google Cloud. You want to validate these policy changes before they are enforced. What service should you use?

* Google Cloud Armor's preconfigured rules in preview mode

1. You are asked to recommend a solution to store and retrieve sensitive configuration data from an application that runs on Compute Engine. Which option should you recommend?

* Secret Manager

1. You need to implement an encryption at-rest strategy that reduces key management complexity for non-sensitive data and protects sensitive data while providing the flexibility of controlling the key residency and rotation schedule. FIPS 140-2 L1 compliance is required for all data types. What should you do?

* Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service.

1. Your company wants to determine what products they can build to help customers improve their credit scores depending on their age range. To achieve this, you need to join user information in the company's banking app with customers' credit score data received from a third party. While using this raw data will allow you to complete this task, it exposes sensitive data, which could be propagated into new systems. This risk needs to be addressed using de-identification and tokenization with Cloud Data Loss Prevention while maintaining the referential integrity across the database. Which cryptographic token format should you use to meet these requirements?

* Deterministic encryption

1. An office manager at your small startup company is responsible for matching payments to invoices and creating billing alerts. For compliance reasons, the office manager is only permitted to have the Identity and Access Management (IAM) permissions necessary for these tasks. Which two IAM roles should the office manager have? (Choose two.)

* Billing Account Viewer
* Billing Account Costs Manager

1. You are designing a new governance model for your organization's secrets that are stored in Secret Manager. Currently, secrets for Production and Non-Production applications are stored and accessed using service accounts. Your proposed solution must:

✑ Provide granular access to secrets

✑ Give you control over the rotation schedules for the encryption keys that wrap your secrets

✑ Maintain environment separation

✑ Provide ease of management Which approach should youtake?

* Use separate Google Cloud projects to store Production and Non-Production secrets. 2. Enforce access control to secrets using project-level identity and Access Management (IAM) bindings. 3. Use customer-managed encryption keys to encrypt secrets

1. You are a security engineer at a finance company. Your organization plans to store data on Google Cloud, but your leadership team is worried about the security of their highly sensitive data Specifically, your company is concerned about internal Google employees' ability to access your company's data on Google Cloud. What solution should you propose?

* Enable Access Transparency logs with Access Approval requests for Google emps.

1. You want to use the gcloud command-line tool to authenticate using a third-party single sign- on (SSO) SAML identity provider. Which options are necessary to ensure that authentication is supported by the third-party identity provider (IdP)? (Choose two.)

* SSO SAML as a third-party IdP and Cloud Identity

1. You work for a large organization where each business unit has thousands of users. You need to delegate management of access control permissions to each business unit. You have the following requirements:

* Each business unit manages access controls for their own proj.
* Each business unit manages access control permissions at scale.
* Business units cannot access other business units' projects.
* Users lose their access if they move to a different business unit or leave the company.

Users and access control permissions are managed by the on-premises directory service. What should you do? (Choose two.)

* Organize projects in folders, and assign permissions to Google groups at the folder level.
* Use Google Cloud Directory Sync to synchronize users and group memberships in Cloud Identity

1. Your organization recently deployed a new application on Google Kubernetes Engine. You need to deploy a solution to protect the application. The solution has the following requirements:

✑ Scans must run at least once per week

✑ Must be able to detect cross-site scripting vulnerabilities

✑ Must be able to authenticate using Google - accounts Which solution should you use?

* Web Security Scanner

108. 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?

* Dedicated Interconnect

109. Your organization has had a few recent DDoS attacks. You need to authenticate responses to domain name lookups. Which Google Cloud service should you use?

* Cloud DNS with DNSSEC

110. Your Security team believes that a former employee of your company gained unauthorized access to Google Cloud resources some time in the past 2 months by using a service account key. You need to confirm the unauthorized access and determine the user activity. What should you do?

* Use the Logs Explorer to search for user activity.

111. Your company requires the security and network engineering teams to identify all n/w anomalies within and across VPCs, internal traffic from VMs to VMs, traffic between end

Loc’s on the internet and VMs, and traffic between VMs to Google Cloud services in production. Which method should you use?

* Configure packet mirroring policies.

112. Your company has been creating users manually in Cloud Identity to provide access to Google Cloud resources. Due to continued growth of the environment, you want to authorize the Google Cloud Directory Sync (GCDS) instance and integrate it with your on-premises LDAP server to onboard hundreds of users. You are required to:

✑ Replicate user and group lifecycle changes from the on-premises LDAP server in Cloud Identity.

✑ Disable any manually created users in Cloud Identity.

You have already configured the LDAP search attributes to include the users and security groups in scope for Google Cloud. What should you do next to complete this solution?

* Configure the option to suspend domain users not found in LDAP. 2. Set up a recurring GCDS task.

113. You are troubleshooting access denied errors between Compute Engine instances connected to a Shared VPC and BigQuery datasets. The datasets reside in a project protected by a VPC Service Controls perimeter. What should you do?

* Add the host project containing the Shared VPC to the service perimeter.

114. You recently joined the networking team supporting your company's Google Cloud implementation. You are tasked with familiarizing yourself with the firewall rules configuration and providing recommendations based on your networking and Google Cloud experience. What product should you recommend to detect firewall rules that are overlapped by attributes from other firewall rules with higher or equal priority?

* Firewall Insights

115. The security operations team needs access to the security-related logs for all projects in their organization. They have the following requirements:

✑ Follow the least privilege model by having only view access to logs.

✑ Have access to Admin Activity logs.

✑ Have access to Data Access logs.

✑ Have access to Access Transparency logs.

Which Identity and Access Management (IAM) role should the security operations team be granted?

* roles/logging.privateLogViewer

116. You are exporting application logs to Cloud Storage. You encounter an error message that the log sinks don't support uniform bucket-level access policies. How should you resolve this error?

* Change the access and control model for the bucket

117.You plan to deploy ur cloud infrastructure using a CI/CD cluster hosted on Compute Engine. You want to minimize the risk of its credentials being stolen by a third party. What should you do?

* Create a custom service account for the cluster. Enable the constraints/iam.disableServiceAccountKeyCreation organization policy at the project lvl

118. You need to set up two network segments: one with an untrusted subnet and the other with a trusted subnet. You want to configure a virtual appliance such as a next-generation firewall (NGFW) to inspect all traffic between the two network segments. How should you design the network to inspect the traffic?

* Set up two VPC networks: one trusted and the other untrusted. 2. Configure a virtual appliance using multiple network interfaces, with each interface connected to one of the VPC networks.

119. You are a member of your company's security team. You have been asked to reduce your Linux bastion host external attack surface by removing all public IP addresses. Site Reliability Engineers (SREs) require access to the bastion host from public locations so they can access the internal VPC while off-site. How should you enable this access?

* Implement Identity-Aware Proxy TCP forwarding for the bastion host

120. u need to enable VPC Service Controls and allow changes to perimeters in existing environments without preventing access to resources. Which VPC Service Controls mode should you use?

* Dry run

121. You manage your organization's Security Operations Center (SOC). You currently monitor and detect network traffic anomalies in your Google Cloud VPCs based on packet header information. However, you want the capability to explore network flows and their payload to aid investigations. Which Google Cloud product should you use?

* Packet Filtering

122. Your organization acquired a new workload. The Web and Application (App) servers will be running on Compute Engine in a newly created custom VPC. You are responsible for configuring a secure network communication solution that meets the following requirements:

✑ Only allows communication between the Web and App tiers.

✑ Enforces consistent network security when autoscaling the Web and App tiers.

✑ Prevents Compute Engine Instance Admins from altering network traffic. What should you do?

* Re-deploy the Web and App servers with instance templates configured with respective service accounts. 2. Create an allow VPC firewall rule that specifies the target/source with respective service accounts.

123. 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?

* 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.

124. You are working with protected health information (PHI) for an electronic health record system. The privacy officer is concerned that sensitive data is stored in the analytics system. You are tasked with anonymizing the sensitive data in a way that is not reversible. Also, the anonymized data should not preserve the character set and length. Which Google Cloud solution should you use?

* Cloud Data Loss Prevention with cryptographic hashing

125. You are setting up a CI/CD pipeline to deploy containerized applications to your production clusters on Google Kubernetes Engine (GKE). You need to prevent containers with known vulnerabilities from being deployed. You have the following requirements for your solution: Must be cloud-native - ✑ Must be cost-efficient ✑ Minimize operational overhead

How should you accomplish this? (Choose two.)

* Create a Cloud Build pipeline that will monitor changes to your container templates in a Cloud Source Repositories repository. Add a step to analyze Container Analysis results before allowing the build to continue.
* In your CI/CD pipeline, add an attestation on your container image when no vulnerabilities have been found. Use a Binary Authorization policy to block deployments of containers with no attestation in your cluster

126. Which type of load balancer should you use to maintain client IP by default while using the standard network tier?

* TCP/UDP Network

127. You want to prevent users from accidentally deleting a Shared VPC host project. Which organization-level policy constraint should you enable?

* compute.restrictXpnProjectLienRemoval

128. Users are reporting an outage on your public-facing application that is hosted on Compute Engine. You suspect that a recent change to your firewall rules is responsible. You need to test whether your firewall rules are working properly. What should you do?

* Enable Firewall Rules Logging on the latest rules that were changed. Use Logs Explorer to analyze whether the rules are working correctly.

129. You are a security administrator at your company. Per Google-recommended best practices, you implemented the domain restricted sharing organization policy to allow only required domains to access your projects. An engineering team is now reporting that users at an external partner outside your organization domain cannot be granted access to the resources in a project. How should you make an exception for your partner's domain while following the stated best practices?

* Turn off the domain restricted sharing organization policy. Set the policy value to "Custom." Add each external partner's Cloud Identity or Google Workspace customer ID as an exception under the organization policy, and then turn the policy back on

130. 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.)

* The backend service's load balancing scheme must be EXTERNAL
* The load balancer must be an external HTTP(S) load balancer.

131. You perform a security assessment on a customer architecture and discover that multiple VMs have public IP addresses. After providing a recommendation to remove the public IP addresses, you are told those VMs need to communicate to external sites as part of the customer's typical operations. What should you recommend to reduce the need for public IP addresses in your customer's VMs?

* Google NAT

132. 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.

* Create a Log Sink at the organization level with the includeChildren parameter, and set the destination to a Pub/Sub topic
* Enable Google Workspace audit logs to be shared with Google Cloud in the Admin Console

133. Your company's Chief Information Security Officer (CISO) creates a requirement that business data must be stored in specific locations due to regulatory requirements that affect the company's global expansion plans. After working on the details to implement this requirement, you determine the following:

✑ The services in scope are included in the Google Cloud Data Residency Terms.

✑ The business data remains within specific locations under the same organization.

✑ The folder structure can contain multiple data residency locations.

You plan to use the Resource Location Restriction organization policy constraint. At which level in the resource hierarchy should you set the constraint?

* Folder

134. You need to set up a Cloud interconnect connection between your company's on-premises data center and VPC host network. You want to make sure that on- premises applications can only access Google APIs over the Cloud Interconnect and not through the public internet. You are required to only use APIs that are supported by VPC Service Controls to mitigate against exfiltration risk to non-supported APIs. How should you configure the network?

* Use restricted googleapis.com to access Google APIs using a set of IP addresses only routable from within Google Cloud, which are advertised as routes over the Cloud Interconnect connection

135. You need to implement an encryption-at-rest strategy that protects sensitive data and reduces key management complexity for non-sensitive data. Your solution has the following requirements:

✑ Schedule key rotation for sensitive data.

✑ Control which region the encryption keys for sensitive data are stored in.

✑ Minimize latency to access encryption keys for both sensitive and non-sensitive data.

* Encrypt non-sensitive data with Google default encryption, and encrypt sensitive data with Cloud Key Management Service

136. Your security team uses encryption keys to ensure confidentiality of user data. You want to establish a process to reduce the impact of a potentially compromised symmetric encryption key in Cloud Key Management Service (Cloud KMS).

Which steps should your team take before an incident occurs? (Choose two.)

* Enable automatic key version rotation on a regular schedule
* Limit the number of messages encrypted with each key version.

137. Your company's chief information security officer (CISO) is requiring business data to be stored in specific locations due to regulatory requirements that affect the company's global expansion plans. After working on a plan to implement this requirement, you determine the following:

✑ The services in scope are included in the Google Cloud data residency requirements.

✑ The business data remains within specific locations under the same organization.

✑ The folder structure can contain multiple data residency locations.

✑ The projects are aligned to specific locations.

You plan to use the Resource Location Restriction organization policy constraint with very granular control. At which level in the hierarchy should you set the constraint?

* Project

138. A database administrator notices malicious activities within their Cloud SQL instance. The database administrator wants to monitor the API calls that read the configuration or metadata of resources. Which logs should the database administrator review?

* Data Access

139. You are backing up application logs to a shared Cloud Storage bucket that is accessible to both the administrator and analysts. Analysts should not have access to logs that contain any personally identifiable information (PII). Log files containing PII should be stored in another bucket that is only accessible to the administrator. What should you do?

* Use Pub/Sub and Cloud Functions to trigger a Cloud Data Loss Prevention scan every time a file is uploaded to the administrator's bucket. If the scan does not detect PII, have the function move the objects into the shared Cloud Storage bucket

140. You work for an organization in a regulated industry that has strict data protection requirements. The organization backs up their data in the cloud. To comply with data privacy regulations, this data can only be stored for a specific length of time and must be deleted after this specific period. You want to automate the compliance with this regulation while minimizing storage costs. What should you do?

* Store the data in a Cloud Storage bucket, and configure the bucket's Object Lifecycle Management feature.

141. You have been tasked with configuring Security Command Center for your organization's Google Cloud environment. Your security team needs to receive alerts of potential crypto mining in the organization's compute environment and alerts for common Google Cloud misconfigurations that impact security. Which Security Command Center features should you use to configure these alerts? (Choose two.)

* Event threat Detection and Security Health Analytics

142. You have noticed an increased number of phishing attacks across your enterprise user accounts. You want to implement the Google 2-Step Verification (2SV) option that uses a cryptographic signature to authenticate a user and verify the URL of the login page. Which Google 2SV option should you use?

* Titan Security Keys

143. 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.

* Configure a VPC peering connection between your organization's VPC network and the third party's that is controlled by VPC firewall rules.

144. Your company's new CEO recently sold two of the company's divisions. Your Director asks you to help migrate the Google Cloud projects associated with those divisions to a new organization node. Which preparation steps are necessary before this migration occurs?

* Create a new folder for all projects to be migrated
* Remove the specific migration projects from any VPC Service Controls perimeters and bridges

145. You are a consultant for an organization that is considering migrating their data from its private cloud to Google Cloud. The organization's compliance team is not familiar with Google Cloud and needs guidance on how compliance requirements will be met on Google Cloud. One specific compliance requirement is for customer data at rest to reside within specific geographic boundaries. Which option should you recommend for the organization to meet their data residency requirements on Google Cloud?

* Organization Policy Service constraints

146. Your security team wants to reduce the risk of user-managed keys being mismanaged and compromised. To achieve this, you need to prevent developers from creating user-managed service account keys for projects in their organization. How should you enforce this?

* Enable an organization policy to prevent service account keys from being created

147. You are responsible for managing your company's identities in Google Cloud. Your company enforces 2-Step Verification (2SV) for all users. You need to reset a user's access, but the user lost their second factor for 2SV. You want to minimize risk. What should you do?

* On the Google Admin console, select the appropriate user account, and generate a backup code to allow the user to sign in. Ask the user to update their second factor

148. Which Google Cloud service should you use to enforce access control policies for applications and resources?

* Identity-Aware Proxy

149. You want to update your existing VPC Service Controls perimeter with a new access level. You need to avoid breaking the existing perimeter with this change, and ensure the least disruptions to users while minimizing overhead. What should you do?

* Enable the dry run mode on your perimeter. Add your new access lvl to the perimeter dry run config. Update the perimeter configuration after the access level has been vetted.

150. 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?

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

151. Your privacy team uses crypto-shredding (deleting encryption keys) as a strategy to delete personally identifiable information (PII). You need to implement this practice on Google Cloud while still utilizing the majority of the platform's services and minimizing operational overhead. What should you do?

* Use customer-managed encryption keys to delete specific encryption keys.

152. You need to centralize your team's logs for production projects. You want your team to be able to search and analyze the logs using Logs Explorer. What should you do?

* Create an aggregate org sink at the parent folder of the production projects, and set the destination to a logs bucket

153. You need to use Cloud External Key Manager to create an encryption key to encrypt specific BigQuery data at rest in Google Cloud. Which steps should you do first?

* Create or use an existing key with a unique uniform resource identifier (URI) in a supported external key management partner system. 2. In the external key management partner system, grant access for this key to use your Google Cloud project.

154. 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?

* Cloud NAT

155. You want to make sure that your organization's Cloud Storage buckets cannot have data publicly available to the internet. You want to enforce this across all Cloud Storage buckets. What should you do?

* Configure uniform bucket-level access, and enforce domain restricted sharing in an organization policy.

156. Your company plans to move most of its IT infrastructure to Google Cloud. They want to leverage their existing on-premises Active Directory as an identity provider for Google Cloud. Which two steps should you take to integrate the company's on-premises Active Directory with Google Cloud and configure access management? (Choose two.)

* Install Google Cloud Directory Sync and connect it to Active Directory and Cloud Identity
* Create Identity and Access Management (IAM) groups with permissions corresponding to each Active Directory group

157. 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?

* Use a physical token to secure the super admin credentials with multi-factor authentication (MFA)
* Provide non-privileged identities to the super admin users for their day-to-day activities

158. You are deploying a web application hosted on Compute Engine. A business requirement mandates that application logs are preserved for 12 years and data is kept within European boundaries. You want to implement a storage solution that minimizes overhead and is cost- effective. What should you do?

* Configure your Compute Engine instances to use the Google Cloud's operations suite Cloud Logging agent to send application logs to a custom log bucket in the EUROPE-WEST1 region with a custom retention of 12 years.

159. You discovered that sensitive personally identifiable information (PII) is being ingested to your Google Cloud environment in the daily ETL process from an on- premises environment to your BigQuery datasets. You need to redact this data to obfuscate the PII, but need to re- identify it for data analytics purposes. Which components should you use in your solution? (Choose two.)

* Cloud Key Management Service
* . Cloud Data Loss Prevention with deterministic encryption using AES-SIV

160. You are working with a client that is concerned about control of their encryption keys for sensitive data. The client does not want to store encryption keys at rest in the same cloud service provider (CSP) as the data that the keys are encrypting. Which Google Cloud encryption solutions should you recommend to this client?

* Customer-supplied encryption keys
* Cloud External Key Manager

161. 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?

* Customer-managed encryption keys

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

* IAP-Secured Web App User

163. 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?

* All VM instances are missing the respective network tags
* 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.

164. 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?

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

165. You are a security administrator at your company and are responsible for managing access controls (identification, authentication, and authorization) on Google

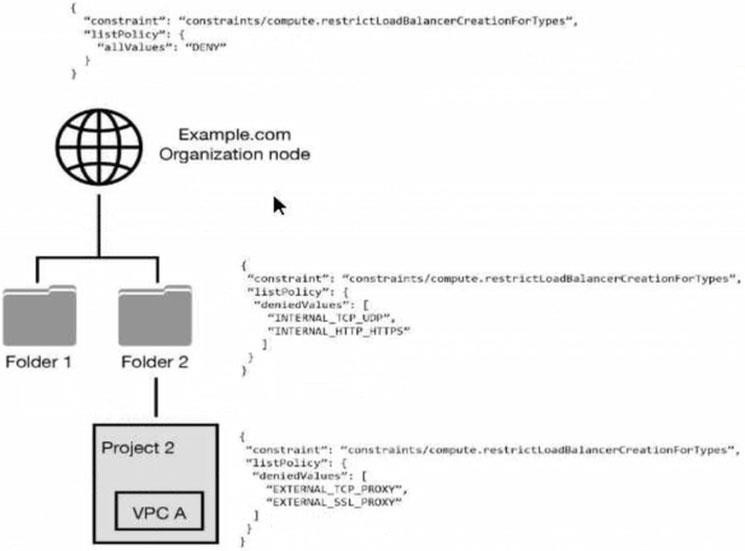
Cloud. Which Google-recommended best practices should you follow when configuring authentication and authorization? (Choose two.)

* Use SSO/SAML integration with Cloud Identity for user authentication and user lifecycle management
* Provide granular access with predefined roles.

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

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

167. 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?



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

168. 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.

* Enable VPC Service Controls, create a perimeter around Projects A and B, and include the Cloud Storage API in the Service Perimeter configuration

169. You need to create a VPC that enables your security team to control network resources such as firewall rules. How should you configure the network to allow for separation of duties for network resources?

* Set up a Shared VPC where the security team manages the firewall rules, and share the network with developers via service projects.

170. You are onboarding new users into Cloud Identity and discover that some users have created consumer user accounts using the corporate domain name. How should you manage these consumer user accounts with Cloud Identity?

* Use the transfer tool for unmanaged user accounts.

171. 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.)

* Grant users the compute.imageUser role in the OS image project
* Set up an image access organization policy constraint, and list the security team managed project in the project's allow list.

172. You're developing the incident response plan for your company. You need to define the access strategy that your DevOps team will use when reviewing and investigating a deployment issue in your Google Cloud environment. There are two main requirements:

✑ Least-privilege access must be enforced at all times.

✑ The DevOps team must be able to access the required resources only during the deployment issue.

How should you grant access while following Google-recommended best practices?

* Create a service account, and grant it limited list/view permissions. Give the Service Account User Role on this service account to the DevOps team. Most Voted

173. 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?

* Customer-managed encryption keys with Cloud HSM

174. 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?

* Packet Mirroring

175. 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.)

* Confidential compuiting and Istio
* Client-side encryption

176. 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?

* Enable the constraints/storage.publicAccessPrevention constraint at the organization level.

177. 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?

* Configure packet mirroring policies

178. You are managing a project for the Business Intelligence (BI) department in your company. A data pipeline ingests data into BigQuery via streaming. You want the users in the BI department to be able to run the custom SQL queries against the latest data in BigQuery.

* Assign the IAM role of BigQuery User to a Google Group that contains the members of the BI team.

179. Your company has a Google Cloud project that uses BigQuery for data warehousing. There are some tables that contain personally identifiable information (PII). Only the compliance team may access the PII. The other information in the tables must be available to the data science team. You want to minimize cost and the time it takes to assign appropriate access to the tables. What should you do?

* Create a dataset for the data science team. 2. Create views of tables that you want to share, excluding PII. 3. Assign an appropriate project-level IAM role to the members of the data science team. 4. Assign access controls to the dataset that contains the view. 5. Authorize the view to access the source dataset