Question: 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.)

A. Public IP
B. IP Forwarding
C. Private Google Access
D. Static routes
E. IAM Network User Role

Answer: AC

Explanation:
Reference:
https://cloud.google.com/vpc/docs/configure-private-google-access

Question: 2

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

A. A rule that allows all outbound connections
B. A rule that denies all inbound connections
C. A rule that blocks all inbound port 25 connections
D. A rule that blocks all outbound connections
E. A rule that allows all inbound port 80 connections

Answer: AB

Explanation:
Reference:
https://cloud.google.com/vpc/docs/firewalls

Question: 3

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?

A. Use Cloud Source Repositories, and store secrets in Cloud SQL.
B. Encrypt the secrets with a Customer-Managed Encryption Key (CMEK), and store them in Cloud Storage.
C. Run the Cloud Data Loss Prevention API to scan the secrets, and store them in Cloud SQL.

D. Deploy the SCM to a Compute Engine VM with local SSDs, and enable preemptible VMs.

Answer: B

Question: 4

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.

Answer: B

Explanation:
Reference:
https://cloud.google.com/blog/products/identity-security/using-your-existing-identity-managementsystem-
with-google-cloud-platform

Question: 5

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

A. Ensure that the app does not run as PID 1.
B. Package a single app as a container.
C. Remove any unnecessary tools not needed by the app.
D. Use public container images as a base image for the app.
E. Use many container image layers to hide sensitive information.

Answer: BC

Explanation:
Reference:
https://cloud.google.com/solutions/best-practices-for-building-containers

Question: 6

A customer needs to launch a 3-tier internal web application on Google Cloud Platform (GCP). The

customer's internal compliance requirements dictate that end-user access may only be allowed if the traffic seems to originate from a specific known good CIDR. The customer accepts the risk that their application will only have SYN flood DDoS protection. They want to use GCP's native SYN flood protection.
Which product should be used to meet these requirements?

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

Answer: A

Explanation:
Reference:
https://cloud.google.com/blog/products/identity-security/understanding-google-cloud-armors-newwaf-capabilities

Question: 7

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.)

A. Configure the project with Cloud VPN.
B. Configure the project with Shared VPC.
C. Configure the project with Cloud Interconnect.
D. Configure the project with VPC peering.
E. Configure all Compute Engine instances with Private Access.

Answer: AC

Explanation:
Reference:
https://cloud.google.com/solutions/secure-data-workloads-use-cases

Question: 8

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 the ERP systems only accept traffic from Cloud Identity- Aware Proxy.
What should the customer do to meet these requirements?

A. Make sure that the ERP system can validate the JWT assertion in the HTTP requests.
B. Make sure that the ERP system can validate the identity headers in the HTTP requests.

C. Make sure that the ERP system can validate the x-forwarded-for headers in the HTTP requests.
D. Make sure that the ERP system can validate the user's unique identifier headers in the HTTP requests.

Answer: A

Question: 9

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?

A. Create an Alerting Policy in Stackdriver using a Process Health condition, checking that the number of executions of the script remains below the desired threshold. Enable notifications.
B. Create an Alerting Policy in Stackdriver using the CPU usage metric. Set the threshold to 80% to be notified when the CPU usage goes above this 80%.
C. Log every execution of the script to Stackdriver Logging. Create a User-defined metric in Stackdriver Logging on the logs, and create a Stackdriver Dashboard displaying the metric.
D. Log every execution of the script to Stackdriver Logging. Configure BigQuery as a log sink, and create a BigQuery scheduled query to count the number of executions in a specific timeframe.

Answer: B

Explanation:
Reference:
https://cloud.google.com/logging/docs/logs-based-metrics/

Question: 10

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?

A. 1. Export logs to a Cloud Pub/Sub topic with folders/NONPROD parent and includeChildren property set to True in a dedicated SIEM project.
2. Subscribe SIEM to the topic.
B. 1. Create a Cloud Storage sink with billingAccounts/ABC-BILLING parent and includeChildren property set to False in a dedicated SIEM project.
2. Process Cloud Storage objects in SIEM.
C. 1. Export logs in each dev project to a Cloud Pub/Sub topic in a dedicated SIEM project.
2. Subscribe SIEM to the topic.
D. 1. Create a Cloud Storage sink with a publicly shared Cloud Storage bucket in each project.
2. Process Cloud Storage objects in SIEM.

Answer: B