PROFESSIONAL-CLOUD-NETWORK-ENGINEER$^{Q\&As}$

Professional Cloud Network Engineer

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

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

QUESTION 1

You deployed a hub-and-spoke architecture in your Google Cloud environment that uses VPC Network Peering to connect the spokes to the hub. For security reasons, you deployed a private Google Kubernetes Engine (GKE) cluster in one of the spoke projects with a private endpoint for the control plane. You configured authorized networks to be the subnet range where the GKE nodes are deployed. When you attempt to reach the GKE control plane from a different spoke project, you cannot access it. You need to allow access to the GKE control plane from the other spoke projects. What should you do?

A. Add a firewall rule that allows port 443 from the other spoke projects.

B. Enable Private Google Access on the subnet where the GKE nodes are deployed.

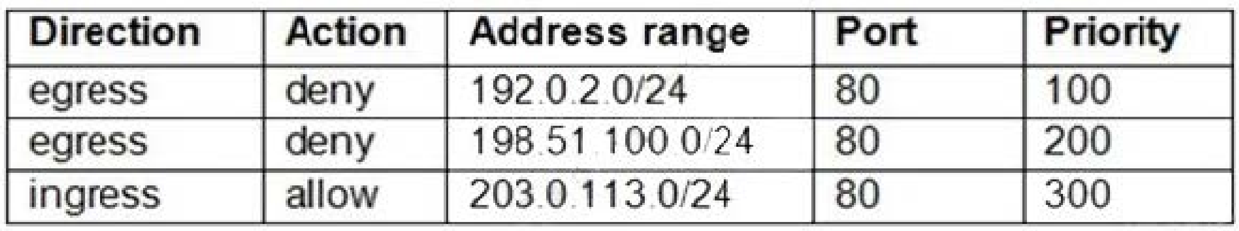
C. Configure the authorized networks to be the subnet ranges of the other spoke projects.

D. Deploy a proxy in the spoke project where the GKE nodes are deployed and connect to the control plane through the proxy.

Correct Answer: C

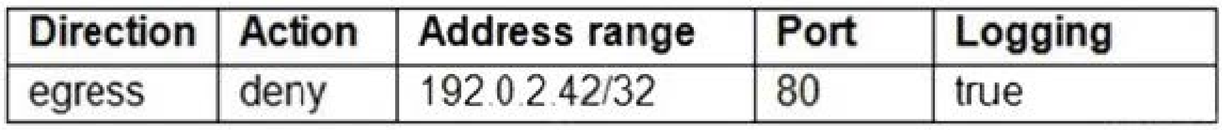
QUESTION 2

You have the following firewall ruleset applied to all instances in your Virtual Private Cloud (VPC):



Direction	Action	Address range	Port	Priority
egress	deny	192.0.2.0/24	80	100
egress	deny	198.51.100.0/24	80	200
ingress	allow	203.0.113.0/24	80	300

You need to update the firewall rule to add the following rule to the ruleset:



Direction	Action	Address range	Port	Logging
egress	deny	192.0.2.42/32	80	true

You are using a new user account. You must assign the appropriate identity and Access Management (IAM) user roles to this new user account before updating the firewall rule. The new user account must be able to apply the update and view firewall logs. What should you do?

A. Assign the compute.securityAdmin and logging.viewer rule to the new user account.Apply the new firewall rule with a priority of 50.

B. Assign the compute.securityAdmin and logging.bucketWriter role to the new user account. Apply the new firewall rule with a priority of 150.

C. Assign the compute.orgSecurityPolicyAdmin and logging.viewer role to the new user account. Apply the new firewall rule with a priority of 50.

D. Assign the compute.orgSecurityPolicyAdmin and logging.bucketWriter role to the new user account. Apply the new firewall rule with a priority of 150.

Correct Answer: A

QUESTION 3

You need to create the network infrastructure to deploy a highly available web application in the us-east1 and us-west1 regions. The application runs on Compute Engine instances, and it does not require the use of a database. You want to follow Google-recommended practices. What should you do?

A. Create one VPC with one subnet in each region. Create a regional network load balancer in each region with a static IP address. Enable Cloud CDN on the load balancers. Create an A record in Cloud DNS with both IP addresses for the load balancers.

B. Create one VPC with one subnet in each region. Create a global load balancer with a static IP address. Enable Cloud CDN and Google Cloud Armor on the load balancer. Create an A record using the IP address of the load balancer in Cloud DNS.

C. Create one VPC in each region, and peer both VPCs. Create a global load balancer. Enable Cloud CDN on the load balancer. Create a CNAME for the load balancer in Cloud DNS.

D. Create one VPC with one subnet in each region. Create an HTTP(S) load balancer with a static IP address. Choose the standard tier for the network. Enable Cloud CDN on the load balancer. Create a CNAME record using the load balancer\\'s IP address in Cloud DNS.

Correct Answer: C

QUESTION 4

You have recently been put in charge of managing identity and access management for your organization. You have several projects and want to use scripting and automation wherever possible. You want to grant the editor role to a project member.

Which two methods can you use to accomplish this? (Choose two.)

A. GetIamPolicy() via REST API

B. setIamPolicy() via REST API

C. gcloud pubsub add-iam-policy-binding Sprojectname --member user:Susername --role roles/editor

D. gcloud projects add-iam-policy-binding Sprojectname --member user:Susername --role roles/editor

E. Enter an email address in the Add members field, and select the desired role from the drop-down menu in the GCP Console.

Correct Answer: DE

QUESTION 5

In your Google Cloud organization, you have two folders: Dev and Prod. You want a scalable and consistent way to enforce the following firewall rules for all virtual machines (VMs) with minimal cost:

Port 8080 should always be open for VMs in the projects in the Dev folder.

Any traffic to port 8080 should be denied for all VMs in your projects in the Prod folder.

What should you do?

A. Create and associate a firewall policy with the Dev folder with a rule to open port 8080. Create and associate a firewall policy with the Prod folder with a rule to deny traffic to port 8080.

B. Create a Shared VPC for the Dev projects and a Shared VPC for the Prod projects. Create a VPC firewall rule to open port 8080 in the Shared VPC for Dev. Create a firewall rule to deny traffic to port 8080 in the Shared VPC for Prod. Deploy VMs to those Shared VPCs.

C. In all VPCs for the Dev projects, create a VPC firewall rule to open port 8080. In all VPCs for the Prod projects, create a VPC firewall rule to deny traffic to port 8080.

D. Use Anthos Config Connector to enforce a security policy to open port 8080 on the Dev VMs and deny traffic to port 8080 on the Prod VMs.

Correct Answer: A

QUESTION 6

You have deployed a new internal application that provides HTTP and TFTP services to on-premises hosts. You want to be able to distribute traffic across multiple Compute Engine instances, but need to ensure that clients are sticky to a particular instance across both services.

Which session affinity should you choose?

A. None

B. Client IP

C. Client IP and protocol

D. Client IP, port and protocol

Correct Answer: B

QUESTION 7

You have configured a service on Google Cloud that connects to an on-premises service via a Dedicated Interconnect. Users are reporting recent connectivity issues. You need to determine whether the traffic is being dropped because of firewall rules or a routing decision. What should you do?

A. Use the Network Intelligence Center Connectivity Tests to test the connectivity between the VPC and the on-premises network.

B. Use Network Intelligence Center Network Topology to check the traffic flow, and replay the traffic from the time period when the connectivity issue occurred.

C. Configure VPC Flow Logs. Review the logs by filtering on the source and destination.

D. Configure a Compute Engine instance on the same VPC as the service running on Google Cloud to run a traceroute targeted at the on-premises service.

Correct Answer: B

QUESTION 8

You need to restrict access to your Google Cloud load-balanced application so that only specific IP addresses can connect.

What should you do?

A. Create a secure perimeter using the Access Context Manager feature of VPC Service Controls and restrict access to the source IP range of the allowed clients and Google health check IP ranges.

B. Create a secure perimeter using VPC Service Controls, and mark the load balancer as a service restricted to the source IP range of the allowed clients and Google health check IP ranges.

C. Tag the backend instances "application," and create a firewall rule with target tag "application" and the source IP range of the allowed clients and Google health check IP ranges.

D. Label the backend instances "application," and create a firewall rule with the target label "application" and the source IP range of the allowed clients and Google health check IP ranges.

Correct Answer: C

https://cloud.google.com/load-balancing/docs/https/setting-up-https#sendtraffic

QUESTION 9

Your company has recently installed a Cloud VPN tunnel between your on-premises data center and your Google Cloud Virtual Private Cloud (VPC). You need to configure access to the Cloud Functions API for your on-premises servers. The configuration must meet the following requirements:

Certain data must stay in the project where it is stored and not be exfiltrated to other projects.

Traffic from servers in your data center with RFC 1918 addresses do not use the internet to access Google Cloud APIs.

All DNS resolution must be done on-premises.

The solution should only provide access to APIs that are compatible with VPC Service Controls.

What should you do?

A. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range. Create a CNAME record for *.googleapis.com that points to the A record. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record. Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.

B. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range. Create a CNAME record for *.googleapis.com that points to the A record. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record. Configure your on-premises firewalls to allow traffic to the restricted.googleapis.com addresses.

C. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range. Create a CNAME record for *.googleapis.com that points to the A record. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record. Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.

D. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range. Create a CNAME record for *.googleapis.com that points to the A record. Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record. Configure your on-premises firewalls to allow traffic to the private.googleapis.com addresses.

Correct Answer: C

QUESTION 10

You recently configured Google Cloud Armor security policies to manage traffic to your application. You discover that Google Cloud Armor is incorrectly blocking some traffic to your application. You need to identity the web application firewall (WAF) rule that is incorrectly blocking traffic. What should you do?

A. Enable firewall logs, and view the logs in Firewall Insights.

B. Enable HTTP(S) Load Balancing logging with sampling rate equal to 1, and view the logs in Cloud Logging.

C. Enable VPC Flow Logs, and view the logs in Cloud Logging.

D. Enable Google Cloud Armor audit logs, and view the logs on the Activity page in the Google Cloud Console.

Correct Answer: A

QUESTION 11

You recently deployed your application in Google Cloud. You need to verify your Google Cloud network configuration before deploying your on-premises workloads. You want to confirm that your Google Cloud network configuration allows traffic to flow from your cloud resources to your on-premises network. This validation should also analyze and diagnose potential failure points in your Google Cloud network configurations without sending any data plane test traffic. What should you do?

A. Use Network Intelligence Center\\'s Connectivity Tests.

B. Enable Packet Mirroring on your application and send test traffic.

C. Use Network Intelligence Center\\'s Network Topology visualizations.

D. Enable VPC Flow Logs and send test traffic.

Correct Answer: C

QUESTION 12

You need to centralize the Identity and Access Management permissions and email distribution for the WebServices Team as efficiently as possible.

What should you do?

A. Create a Google Group for the WebServices Team.

B. Create a G Suite Domain for the WebServices Team.

C. Create a new Cloud Identity Domain for the WebServices Team.

D. Create a new Custom Role for all members of the WebServices Team.

Correct Answer: A

QUESTION 13

You have just deployed your infrastructure on Google Cloud. You now need to configure the DNS to meet the following requirements:

Your on-premises resources should resolve your Google Cloud zones.

Your Google Cloud resources should resolve your on-premises zones.

You need the ability to resolve ". internal" zones provisioned by Google Cloud.

What should you do?

A. Configure an outbound server policy, and set your alternative name server to be your on-premises DNS resolver. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google\\'s public DNS 8.8.8.8.

B. Configure both an inbound server policy and outbound DNS forwarding zones with the target as the on-premises DNS resolver. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google Cloud\\'s DNS resolver.

C. Configure an outbound DNS server policy, and set your alternative name server to be your on-premises DNS resolver. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google Cloud\\'s DNS resolver.

D. Configure Cloud DNS to DNS peer with your on-premises DNS resolver. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google\\'s public DNS 8.8.8.8.

Correct Answer: A

QUESTION 14

Your team is developing an application that will be used by consumers all over the world. Currently, the application sits behind a global external application load balancer You need to protect the application from potential application-level attacks. What should you do?

A. Enable Cloud CDN on the backend service.

B. Create multiple firewall deny rules to block malicious users, and apply them to the global external application load balancer

C. Create a Google Cloud Armor security policy with web application firewall rules, and apply the security policy to the backend service.

D. Create a VPC Service Controls perimeter with the global external application load balancer as the protected service, and apply it to the backend service

Correct Answer: C

The correct answer is C because it meets the requirement of protecting the application from potential application-level attacks. Google Cloud Armor security policies are sets of rules that match on attributes from Layer 3 to Layer 7 to protect externally facing applications1. Web application firewall (WAF) rules are predefined rules that detect and mitigate common web attacks such as cross-site scripting (XSS), SQL injection, remote file inclusion, and more2. By applying a Google Cloud Armor security policy with WAF rules to the backend service, you can filter out malicious requests before they reach your application. Option A is incorrect because Cloud CDN is a content delivery network that caches static content at the edge of Google\\'s network, but it does not provide any protection against application-level attacks3. Option B is incorrect because firewall rules are applied at the VPC network level, not at the load balancer level4. Firewall rules also only match on Layer 3 and 4 attributes, not on Layer 7 attributes that are relevant for application-level attacks4. Option D is incorrect because VPC Service Controls perimeter is a feature that helps you secure your data from unauthorized access by users outside your organization, but it does not protect your application from external attacks. References: Security policy overview | Google Cloud Armor Web application firewall (WAF) rules | Google Cloud Armor Cloud CDN overview | Google Cloud Using firewall rules | VPC [VPC Service Controls overview | Google Cloud]

QUESTION 15

You want to set up two Cloud Routers so that one has an active Border Gateway Protocol (BGP) session, and the other one acts as a standby.

Which BGP attribute should you use on your on-premises router?

A. AS-Path

B. Community

C. Local Preference

D. Multi-exit Discriminator

Correct Answer: D