Free Questions for Professional-Cloud-Network-Engineer by braindumpscollection

Shared by Anthony on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Your company has provisioned 2000 virtual machines (VMs) in the private subnet of your Virtual Private Cloud (VPC) in the us-east1 region. You need to configure each VM to have a minimum of 128 TCP connections to a public repository so that users can download software updates and packages over the internet. You need to implement a Cloud NAT gateway so that the VMs are able to perform outbound NAT to the internet. You must ensure that all VMs can simultaneously connect to the public repository and download software updates and packages. Which two methods can you use to accomplish this? (Choose two.)

Options:

A- Configure the NAT gateway in manual allocation mode, allocate 2 NAT IP addresses, and update the minimum number of ports per VM to 256.

B- Create a second Cloud NAT gateway with the default minimum number of ports configured per VM to 64.

C- Use the default Cloud NAT gateway's NAT proxy to dynamically scale using a single NAT IP address.

D- Use the default Cloud NAT gateway to automatically scale to the required number of NAT IP addresses, and update the minimum number of ports per VM to 128.

E- Configure the NAT gateway in manual allocation mode, allocate 4 NAT IP addresses, and update the minimum number of ports per VM to 128.

Answer:

A, B

Question 2

Question Type: MultipleChoice

Your organization has a single project that contains multiple Virtual Private Clouds (VPCs). You need to secure API access to your Cloud Storage buckets and BigQuery datasets by allowing API access only from resources in your corporate public networks. What should you do?

Options:

A- Create an access context policy that allows your VPC and corporate public network IP ranges, and then attach the policy to Cloud Storage and BigQuery.

B- Create a VPC Service Controls perimeter for your project with an access context policy that allows your corporate public network IP ranges.

C- Create a firewall rule to block API access to Cloud Storage and BigQuery from unauthorized networks.

D- Create a VPC Service Controls perimeter for each VPC with an access context policy that allows your corporate public network IP ranges.

Answer:

B

Question 3

Question Type: MultipleChoice

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?

Options:

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.

Answer:

A

Question 4

Question Type: **MultipleChoice**

You are designing a hybrid cloud environment. Your Google Cloud environment is interconnected with your on-premises network using HA VPN and Cloud Router in a central transit hub VPC. The Cloud Router is configured with the default settings. Your on-premises DNS server is located at 192.168.20.88. You need to ensure that your Compute Engine resources in multiple spoke VPCs can resolve on-premises private hostnames using the domain corp.altostrat.com while also resolving Google Cloud hostnames. You want to follow

Google-recommended practices. What should you do?

Options:

A- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
Associate the zone with the hub VPC.
Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.
Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
Configure VPC peering in the spoke VPCs to peer with the hub VPC.

B- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
Associate the zone with the hub VPC. Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke PCs, with the hub VPC as the target.
Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.

C- Create a private forwarding zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com that points to 192.168.20.88.
Associate the zone with the hub VPC.
Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the hub VPC as the target.
Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
Create a hub-and-spoke VPN deployment in each spoke VPC to connect back to the on-premises network directly.

D- Create a private forwarding zone in Cloud DNS for 'corp altostrat.com' called corp-altostrat-com that points to 192. 168.20.88.
Associate the zone with the hub VPC.
Create a private peering zone in Cloud DNS for 'corp.altostrat.com' called corp-altostrat-com associated with the spoke VPCs, with the

hub VPC as the target.
Sat a custom route advertisement on the Cloud Router for 35.199.192.0/19.
Create a hub and spoke VPN deployment in each spoke VPC to connect back to the hub VPC.

Answer:

A

Question 5

Question Type: MultipleChoice

You successfully provisioned a single Dedicated Interconnect. The physical connection is at a colocation facility closest to us-west2. Seventy-five percent of your workloads are in us-east4, and the remaining twenty-five percent of your workloads are in us-central1. All workloads have the same network traffic profile. You need to minimize data transfer costs when deploying VLAN attachments. What should you do?

Options:

A- Keep the existing Dedicated interconnect. Deploy a VLAN attachment to a Cloud Router in us-west2, and use VPC global routing to access workloads in us-east4 and us-central1.

B- Keep the existing Dedicated Interconnect. Deploy a VLAN attachment to a Cloud Router in us-east4, and deploy another VLAN

attachment to a Cloud Router in us-central1.

C- Order a new Dedicated Interconnect for a colocation facility closest to us-east4, and use VPC global routing to access workloads in us-central1.

D- Order a new Dedicated Interconnect for a colocation facility closest to us-central1, and use VPC global routing to access workloads in us-east4.

Answer:

C

Question 6

Question Type: **MultipleChoice**

Your company's security team wants to limit the type of inbound traffic that can reach your web servers to protect against security threats. You need to configure the firewall rules on the web servers within your Virtual Private Cloud (VPC) to handle HTTP and HTTPS web traffic for TCP only. What should you do?

Options:

A- Create an allow on match ingress firewall rule with the target tag "web-server" to allow all IP addresses for TCP port 80.

B- Create an allow on match egress firewall rule with the target tag "web-server'' to allow all IP addresses for TCP port 80.

C- Create an allow on match ingress firewall rule with the target tag "web-server'' to allow all IP addresses for TCP ports 80 and 443.

D- Create an allow on match egress firewall rule with the target tag "web-server' to allow web server IP addresses for TCP ports 60 and 443.

Answer:

C