Professional Cloud Network Engineer

1. 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.

Answer(s): C

---

2. Your end users are located in close proximity to us-east1 and europe-west1. Their workloads need to communicate with each other. You want to minimize cost and increase network efficiency. How should you design this topology?

A. Create 2 VPCs, each with their own regions and individual subnets. Create 2 VPN gateways to establish connectivity between these regions.

B. Create 2 VPCs, each with their own region and individual subnets. Use external IP addresses on the instances to establish connectivity between these regions.

C. Create 1 VPC with 2 regional subnets. Create a global load balancer to establish connectivity between the regions.

D. Create 1 VPC with 2 regional subnets. Deploy workloads in these subnets and have them communicate using private RFC1918 IP addresses.

Answer(s): D

3. Your organization is deploying a single project for 3 separate departments. Two of these departments require network connectivity between each other, but the third department should remain in isolation. Your design should create separate network administrative domains between these departments. You want to minimize operational overhead.
How should you design the topology?

A. Create a Shared VPC Host Project and the respective Service Projects for each of the 3 separate departments.

B. Create 3 separate VPCs, and use Cloud VPN to establish connectivity between the two appropriate VPCs.

C. Create 3 separate VPCs, and use VPC peering to establish connectivity between the two appropriate VPCs.

D. Create a single project, and deploy specific firewall rules. Use network tags to isolate access between the departments.

Answer(s): C

---

4. You are migrating to Cloud DNS and want to import your BIND zone file.
Which command should you use?

A. gcloud dns record-sets import ZONE_FILE --zone MANAGED_ZONE

B. gcloud dns record-sets import ZONE_FILE --replace-origin-ns --zone MANAGED_ZONE

C. gcloud dns record-sets import ZONE_FILE --zone-file-format --zone MANAGED_ZONE

D. gcloud dns record-sets import ZONE_FILE --delete-all-existing --zone MANAGED ZONE

Answer(s): C

---

5. You created a VPC network named Retail in auto mode. You want to create a VPC network named Distribution and peer it with the Retail VPC.
How should you configure the Distribution VPC?

A. Create the Distribution VPC in auto mode. Peer both the VPCs via network peering.

B. Create the Distribution VPC in custom mode. Use the CIDR range 10.0.0.0/9. Create the necessary subnets, and then peer them via network peering.

C. Create the Distribution VPC in custom mode. Use the CIDR range 10.128.0.0/9. Create the necessary subnets, and then peer them via network peering.

D. Rename the default VPC as "Distribution" and peer it via network peering.

Answer(s): B

---

6. You are using a third-party next-generation firewall to inspect traffic. You created a custom route of 0.0.0.0/0 to route egress traffic to the firewall. You want to allow your VPC instances without public IP addresses to access the BigQuery and Cloud Pub/Sub APIs, without sending the traffic through the firewall.
Which two actions should you take? (Choose two.)

- [ ] A. Turn on Private Google Access at the subnet level.
- [ ] B. Turn on Private Google Access at the VPC level.
- [ ] C. Turn on Private Services Access at the VPC level.
- [ ] D. Create a set of custom static routes to send traffic to the external IP addresses of Google APIs and services via the default internet gateway.
- [ ] E. Create a set of custom static routes to send traffic to the internal IP addresses of Google APIs and services via the default internet gateway.

Answer(s): A D

---

7. All the instances in your project are configured with the custom metadata enable-oslogin value set to FALSE and to block project-wide SSH keys. None of the instances are set with any SSH key, and no project-wide SSH keys have been configured. Firewall rules are set up to allow SSH sessions from any IP address range. You want to SSH into one instance.
What should you do?

A. Open the Cloud Shell SSH into the instance using gcloud compute ssh.

B. Set the custom metadata enable-oslogin to TRUE, and SSH into the instance using a third-party tool like putty or ssh.

C. Generate a new SSH key pair. Verify the format of the private key and add it to the instance. SSH into the instance using a third-party tool like putty or ssh.

D. Generate a new SSH key pair. Verify the format of the public key and add it to the project. SSH into the instance using a third-party tool like putty or ssh.

Answer(s): A

---

8. You work for a university that is migrating to GCP.
These are the cloud requirements:
· On-premises connectivity with 10 Gbps
· Lowest latency access to the cloud
· Centralized Networking Administration Team
New departments are asking for on-premises connectivity to their projects. You want to deploy the most cost-efficient interconnect solution for connecting the campus to Google Cloud.
What should you do?

A. Use Shared VPC, and deploy the VLAN attachments and Interconnect in the host project.

B. Use Shared VPC, and deploy the VLAN attachments in the service projects. Connect the VLAN attachment to the Shared VPC's host project.

C. Use standalone projects, and deploy the VLAN attachments in the individual projects. Connect the VLAN attachment to the standalone projects' Interconnects.

D. Use standalone projects and deploy the VLAN attachments and Interconnects in each of the individual projects.

Answer(s): A

---

9. 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

Answer(s): B

---

10. You created a new VPC network named Dev with a single subnet. You added a firewall rule for the network Dev to allow HTTP traffic only and enabled logging.
When you try to log in to an instance in the subnet via Remote Desktop Protocol, the login fails. You look for the Firewall rules logs in Stackdriver Logging, but you do not see any entries for blocked traffic. You want to see the logs for blocked traffic.
What should you do?

A. Check the VPC flow logs for the instance.

B. Try connecting to the instance via SSH, and check the logs.

C. Create a new firewall rule to allow traffic from port 22, and enable logs.

D. Create a new firewall rule with priority 65500 to deny all traffic, and enable logs.

Answer(s): D

---

11. You are trying to update firewall rules in a shared VPC for which you have been assigned only Network Admin permissions. You cannot modify the firewall rules. Your organization requires using the least privilege necessary.
Which level of permissions should you request?

A. Security Admin privileges from the Shared VPC Admin.

B. Service Project Admin privileges from the Shared VPC Admin.

C. Shared VPC Admin privileges from the Organization Admin.

D. Organization Admin privileges from the Organization Admin.

Answer(s): A

---

12. You want to create a service in GCP using IPv6.
What should you do?

A. Create the instance with the designated IPv6 address.

B. Configure a TCP Proxy with the designated IPv6 address.

C. Configure a global load balancer with the designated IPv6 address.

D. Configure an internal load balancer with the designated IPv6 address.

Answer(s): C

---

13. You want to deploy a VPN Gateway to connect your on-premises network to GCP. You are using a non BGP-capable on-premises VPN device. You want to minimize downtime and operational overhead when your network grows. The device supports only IKEv2, and you want to follow Google- recommended practices.
What should you do?

A. · Create a Cloud VPN instance.· Create a policy-based VPN tunnel per subnet.· Configure the appropriate local and remote traffic selectors to match your local and remote networks.· Create the appropriate static routes.

B. · Create a Cloud VPN instance.· Create a policy-based VPN tunnel.· Configure the appropriate local and remote traffic selectors to match your local and remote networks.· Configure the appropriate static routes.

C. · Create a Cloud VPN instance.· Create a route-based VPN tunnel.· Configure the appropriate local and remote traffic selectors to match your local and remote networks.· Configure the appropriate static routes.

D. · Create a Cloud VPN instance.· Create a route-based VPN tunnel.· Configure the appropriate local and remote traffic selectors to 0.0.0.0/0.· Configure the appropriate static routes.

Answer(s): B

---

14. Your company just completed the acquisition of Altostrat (a current GCP customer). Each company has a separate organization in GCP and has implemented a custom DNS solution. Each organization will retain its current domain and host names until after a full transition and architectural review is done in one year. These are the assumptions for both GCP environments.
· Each organization has enabled full connectivity between all of its projects by using Shared VPC.
· Both organizations strictly use the 10.0.0.0/8 address space for their instances, except for bastion hosts (for accessing the instances) and load balancers for serving web traffic. · There are no prefix overlaps between the two organizations. · Both organizations already have firewall rules that allow all inbound and outbound traffic from the 10.0.0.0/8 address space.
· Neither organization has Interconnects to their on-premises environment.
You want to integrate networking and DNS infrastructure of both organizations as quickly as possible and with minimal downtime.
Which two steps should you take? (Choose two.)

- [ ] A. Provision Cloud Interconnect to connect both organizations together.
- [ ] B. Set up some variant of DNS forwarding and zone transfers in each organization.
- [ ] C. Connect VPCs in both organizations using Cloud VPN together with Cloud Router.
- [ ] D. Use Cloud DNS to create A records of all VMs and resources across all projects in both organizations.
- [ ] E. Create a third organization with a new host project, and attach all projects from your company and Altostrat to it using shared VPC.

Answer(s): B C

---

15. Your on-premises data center has 2 routers connected to your Google Cloud environment through a VPN on each router. All applications are working correctly; however, all of the traffic is passing across a single VPN instead of being load-balanced across the 2 connections as desired. During troubleshooting you find:
· Each on-premises router is configured with a unique ASN. · Each on-premises router is configured with the same routes and priorities. · Both on-premises routers are configured with a VPN connected to a single Cloud Router. · BGP sessions are established between both on-premises routers and the Cloud Router. · Only 1 of the on-premises router's routes are being

added to the routing table.
What is the most likely cause of this problem?

A. The on-premises routers are configured with the same routes.

B. A firewall is blocking the traffic across the second VPN connection.

C. You do not have a load balancer to load-balance the network traffic.

D. The ASNs being used on the on-premises routers are different.

Answer(s): D

---

16. You have ordered Dedicated Interconnect in the GCP Console and need to give the Letter of Authorization/Connecting Facility Assignment (LOA-CFA) to your cross-connect provider to complete the physical connection.
Which two actions can accomplish this? (Choose two.)

- [ ] A. Open a Cloud Support ticket under the Cloud Interconnect category.
- [ ] B. Download the LOA-CFA from the Hybrid Connectivity section of the GCP Console.
- [ ] C. Run gcloud compute interconnects describe .
- [ ] D. Check the email for the account of the NOC contact that you specified during the ordering process.
- [ ] E. Contact your cross-connect provider and inform them that Google automatically sent the LOA/CFA to them via email, and to complete the connection.

Answer(s): D E

---

17. Your company offers a popular gaming service. Your instances are deployed with private IP addresses, and external access is granted through a global load balancer. You believe you have identified a potential malicious actor, but aren't certain you have the correct client IP address. You want to identify this actor while minimizing disruption to your legitimate users.
What should you do?

A. Create a Cloud Armor Policy rule that denies traffic and review necessary logs.

B. Create a Cloud Armor Policy rule that denies traffic, enable preview mode, and review necessary logs.

C. Create a VPC Firewall rule that denies traffic, enable logging and set enforcement to disabled, and review necessary logs.

D. Create a VPC Firewall rule that denies traffic, enable logging and set enforcement to enabled, and review necessary logs.

Answer(s): B

---

18. Your company's web server administrator is migrating on-premises backend servers for an application to GCP. Libraries and configurations differ significantly across these backend servers. The migration to GCP will be lift-and-shift, and all requests to the servers will be served by a single network load balancer frontend. You want to use a GCP-native solution when possible. How should you deploy this service in GCP?

A. Create a managed instance group from one of the images of the on-premises servers, and link this instance group to a target pool behind your load balancer.

B. Create a target pool, add all backend instances to this target pool, and deploy the target pool behind your load balancer.

C. Deploy a third-party virtual appliance as frontend to these servers that will accommodate the significant differences between these backend servers.

D. Use GCP's ECMP capability to load-balance traffic to the backend servers by installing multiple equal-priority static routes to the backend servers.

Answer(s): B

---

19. You decide to set up Cloud NAT. After completing the configuration, you find that one of your instances is not using the Cloud NAT for outbound NAT.
What is the most likely cause of this problem?

A. The instance has been configured with multiple interfaces.

B. An external IP address has been configured on the instance.

C. You have created static routes that use RFC1918 ranges.

D. The instance is accessible by a load balancer external IP address.

Answer(s): B

---

20. 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

Answer(s): D
