1. You are designing a new VPC network that will route traffic to networks in your company’s private data center. You want to ensure that your VPC can support high availability in the future. The data center team requires you to use a routing protocol that can dynamically fail over if there is a link failure in the data center. Your management requires your design to use only native cloud services. Which routing protocol should you use?
A. BGP
B. RIP
C. OSPF
D. Static routing

2. Your new project currently requires 5 gigabits per second (Gbps) of egress traffic from your Google Cloud environment to your company’s private data center, but may scale up to 80 Gbps of traffic in the future. You do not have any public addresses to use. Your company is looking for the most cost-effective long-term solution. Which type of connection should you use?
A. Carrier Peering
B. Partner Interconnect
C. Dedicated Interconnect
D. A single Virtual Private Network (VPN) tunnel

3. Your company just moved to GCP. You configured separate VPC networks for the Finance and Sales departments. Finance needs access to some resources that are part of the Sales VPC. You want to allow the private RFC 1918 address space traffic to flow between Sales and Finance VPCs without any additional cost and without compromising the security or performance. What should you do?

A. Create a VPN tunnel between the two VPCs.
B. Configure VPC peering between the two VPCs.
C. Add a route on both VPCs to route traffic over the internet.
D. Create an Interconnect connection to access the resources.

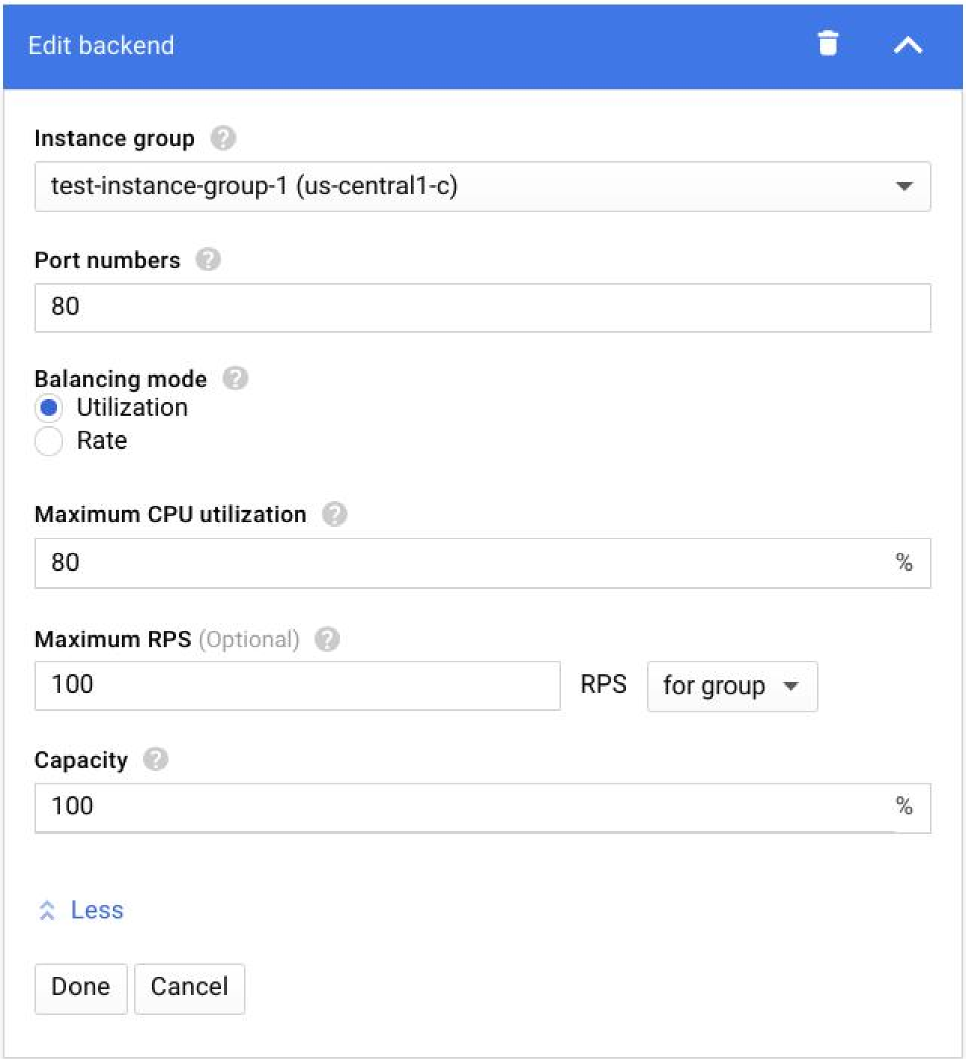
4. You created two subnets named Test and Web in the same VPC network. You enabled VPC Flow Logs for the Web subnet. You are trying to connect instances in the Test subnet to the web servers running in the Web subnet, but all of the connections are failing. You do not see any entries in the Stackdriver logs. What should you do?
A. Enable VPC Flow Logs for the Test subnet also.
B. Make sure that there is a valid entry in the route table.
C. Add a firewall rule to allow traffic from the Test subnet to the Web subnet.
D. Create a subnet in another VPC, and move the web servers in the new subnet.

5. You need to configure a static route as a backup to an existing static route. You want to ensure that the new route is only used when the existing route is no longer available. What should you do?
A. Create a network tag with a value of backup for the new static route.
B. Set a lower priority value for the new static route than the existing static route.
C. Set a higher priority value for the new static route than the existing static route.
D. Configure the same priority value for the new static route as the existing static route.

6. You are configuring the backend service for a new Google Cloud HTTPS load balancer. The application requires high availability and multiple subnets and needs to scale automatically. Which backend configuration should you choose?
A. A Zonal Managed Instance Group
B. A Regional Managed Instance Group
C. An Unmanaged Instance Group

D. A Network Endpoint Group

7. You have the Google Cloud load balancer backend configuration shown below. You want to reduce your instance group utilization by 20%. Which settings should you use?



Instance group: test-instance-group-1 (us-central1-c)

Port numbers: 80

Balancing mode
● Utilization
○ Rate

Maximum CPU utilization: 80 %

Maximum RPS (Optional): 100 RPS for group

Capacity: 100 %

A. Maximum CPU utilization: 60 and Maximum RPS: 80
B. Maximum CPU utilization: 80 and Capacity: 80
C. Maximum RPS: 80 and Capacity: 80
D. Maximum CPU: 60, Maximum RPS: 80, and Capacity: 80

8. You are configuring a hybrid cloud topology for your organization. You are using Cloud VPN and Cloud Router to establish connectivity to your on-premises environment. You need to transfer data from on-premises to a Cloud Storage bucket and to BigQuery. Your organization has a strict security policy that mandates the use of VPN for communication to the cloud. You want to follow Google-recommended practices. What should you do?

A. Create an instance in your VPC with Private Google Access enabled. Transfer data using your VPN connection to the instance in your VPC. Use “gsutil cp files gs://bucketname” and “bq --location=[LOCATION] load --source_format=[FORMAT]

[DATASET].[TABLE] [PATH_TO_SOURCE] [SCHEMA]” on the instance to transfer data to Cloud Storage and BigQuery.
B. Use “nslookup -q=TXT _spf.google.com” to obtain the API IP endpoints used for Cloud Storage and BigQuery from Google’s netblock. Configure Cloud Router to advertise these netblocks to your on-premises router using a flexible routing advertisement. Use “gsutil cp files gs://bucketname” and “bq --location=[LOCATION] load --source_format=[FORMAT] [DATASET].[TABLE] [PATH_TO_SOURCE] [SCHEMA]” on-premises to transfer data to Cloud Storage and BigQuery.
C. Configure Cloud Router to advertise 199.36.153.4/30 to your on-premises router using a flexible routing advertisement. Modify your on-premises DNS server CNAME entry from *.googleapis.com to restricted.googleapis.com. Use “gsutil cp files gs://bucketname and bq --location=[LOCATION] load --source_format=[FORMAT] [DATASET].[TABLE] [PATH_TO_SOURCE] [SCHEMA]” on-premises to transfer data to Cloud Storage and BigQuery.
D. Use “gsutil cp files gs://bucketname” and “bq --location=[LOCATION] load --source_format=[FORMAT] [DATASET].[TABLE] [PATH_TO_SOURCE] [SCHEMA]” on-premises to transfer data to Cloud Storage and BigQuery.

9. You work for a university that is migrating to GCP. You are part of a centralized networking administration team. You require on-premises connectivity with 10 Gbps and lowest-latency access to the cloud. Several applications need to be lifted and shifted with hard-coded IP addresses.You want to connect a small remote campus location that has multiple CIDR ranges to the Cloud using an on-premises BGP-capable VPN Gateway across a public internet link. The on-premises Gateway only supports IKEv1 and has a throughput requirement of up to 3 Gbps. You want to follow Google-recommended practices. What should you do?

A. Create 1 Cloud VPN instance. Create 1 tunnel toward the VPN Gateway using a route-based VPN. Set the traffic selectors to 0.0.0.0/0. Configure routes to point to the on-premises remote campus CIDR ranges.
B. Create 1 Cloud VPN instance. Create 1 tunnel toward the VPN Gateway using a policy-based VPN. Set the local traffic selectors to the GCP ranges, and set the remote traffic selectors to the on-premises ranges.
C. Create 2 Cloud VPN instances. Create a Cloud Router. Create a Dynamic VPN tunnel per instance toward the VPN Gateway. Configure routes to exchange between the on-premises remote campus and GCP.
D. Create 2 Cloud VPN instances. Create 2 tunnels toward the VPN Gateway using a policy-based VPN. Set the local traffic selectors to the GCP ranges, and set the remote traffic selectors to the on-premises ranges on both tunnels.

10. You are using a single Cloud Router to exchange routes between your VPC and on-premises network with Dedicated Interconnect. You want to make sure you can still forward traffic, even if all the Cloud Routers in a region go down. What should you do?

A. Use static routes as a backup to Cloud Router.
B. Turn on graceful restart on your on-premises router.
C. Turn on global routing in your VPC, and create another Cloud Router in a different region.
D. Create a second Cloud Router in the same region, but with a Border Gateway Protocol (BGP) session to a second on-premises device.

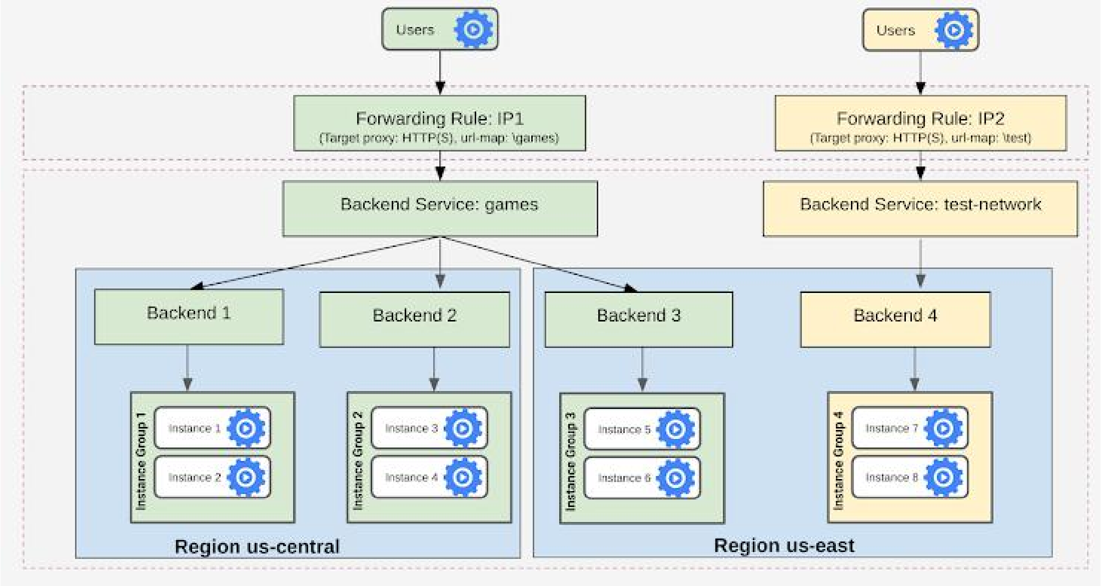
11. You work on a centralized network administration team for a multinational enterprise that is moving to GCP. Your company has on-premises data centers located in the United States in Oregon and New York, with dedicated interconnects to cloud regions us-west1 and us-east4. There are multiple regional offices in Europe and APAC and regional data processing in europe-west1 and australia-southeast1. You want to configure your Cloud Routers so that data from the US data centers can be processed by Compute Engine instances in regional offices in London, UK and Sydney, Australia. How should you configure the topology?

A. Create Cloud Routers using regional routing in region europe-west1 and australia-southeast1. Create a VLAN attachment from the Interconnects pointing to the Cloud Router in europe-west1 and australia-southeast1. Advertise appropriate routes from both region europe-west1 and australia-southeast1 to your on-premises environment.
B. Create Cloud Routers using global routing in region europe-west1 and australia-southeast1. Create a VLAN attachment from the Interconnects pointing to the Cloud Router in europe-west1 and australia-southeast1. Advertise appropriate routes from both region europe-west1 and australia-southeast1 to your on-premises environment.
C. Create Cloud Routers using global routing in region us-west1 and us-east4. Create a VLAN attachment from the Interconnects pointing to the Cloud Router in us-west1 and us-east4. Advertise appropriate routes from both region europe-west1 and australia-southeast1 to your on-premises environment.
D. Create Cloud Routers using regional routing in region us-west1 and us-east4. Create a VLAN attachment from the Interconnects pointing to the Cloud Router in us-west1 and us-east4. Advertise appropriate routes from both region europe-west1 and australia-southeast1 to your on-premises environment.

12. Your manager has asked for a list of all Custom Roles with stage General Availability within Identity Access Management. What should you do?

A. From the GCloud Command line, run "gcloud iam list-testable-permissions".
B. From the GCloud Command line, run "gcloud iam roles list --project vpcuser09project".
C. Open the IAM Console and sort Custom Roles. Gather the required information from the Status Field.
D. Open the IAM Console and sort Custom Roles. Gather the required information from the Permissions Field.

13. Your company offers a popular gaming service. The service architecture is shown in the diagram below. Your instances are deployed with private IP addresses, and external access is granted through a global load balancer. Your application team wants to expose their test environment to select users outside your organization. You want to integrate the test environment into your existing deployment to reduce management overhead and restrict access to only select users. What should you do?



A. Create a new load balancer, and update VPC Firewall rules to allow test clients.
B. Create a new load balancer, and update the VPC Service Controls Perimeter to allow test clients.
C. Add the backend service to the existing load balancer, and modify the existing Cloud Armor policy.
D. Add the backend service to the existing load balancer, and add a new Cloud Armor policy and target test-network.

14. Your company uses a physical security appliance for intrusion detection in its on-premises data center. Your company wants to collect telemetry data using a VPN that connects the GCP environment with the on-premises data center. You want to implement a solution that will integrate the GCP environment and transfer telemetry data to the on-premises physical security appliance as quickly and effectively as possible. What should you do?

A. Set up iptables in all Compute Engine instances in GCP to track connection sessions.
B. Route all traffic in the GCP environment to on-premises for inspection before forwarding back to GCP.
C. Write a script that uses Stackdriver and GCP network logging information to collect and analyze monitoring data for intrusion detection.
D. Deploy a GCP Marketplace virtual security appliance from the same vendor with a multi-nic instance, and grant the security team access to configure the instance as needed.

15. You have a Dedicated Interconnect with two 10-Gbps links. You want to create a Stackdriver alerting policy that will notify you if either of the two links goes down. Which alerts should you add to the policy?

A. An alert for when the Circuit Operational Status metric threshold for either circuit falls below 1.
B. An alert for when the Interconnect Operational Status metric threshold for the interconnect falls below 1.
C. An alert for when the Interconnect Network Capacity metric threshold for the interconnect falls below 20.
D. An alert for when the Interconnect Dropped Packets metric threshold for the interconnect goes above 0.

16. You want to allow access over ports 80 and 443 to servers with the tag "webservers" from external addresses. Currently, there is a firewall rule with priority of 1000 that denies all incoming traffic from an external address on all ports and protocols. You want to allow the desired traffic without deleting the existing rule. What should you do?

A. Add an ingress rule that allows traffic over ports 80 and 443 from any external address in the rules prior to the deny statement.
B. Add an ingress rule that allows traffic over ports 80 and 443 from any external address to the target network tag "webservers" with a priority value of 500.
C. Add an egress rule that allows traffic over ports 80 and 443 from any external address in the rules prior to the deny statement.
D. Add an egress rule that allows traffic over ports 80 and 443 from any external address to the target network tag "webservers" with a priority value of 1500.

17. One of the secure web applications in your GCP project is currently only serving users in North America. All of the application's resources are currently hosted in a single GCP region. The application uses a large catalog of graphical assets from a Cloud Storage bucket. You are notified that the application now needs to serve global clients without adding any additional GCP regions or Compute Engine instances. What should you do?

A. Configure Cloud CDN.
B. Configure a TCP Proxy.
C. Configure a Network load balancer.
D. Configure Dynamic Routing for the subnet hosting the application.

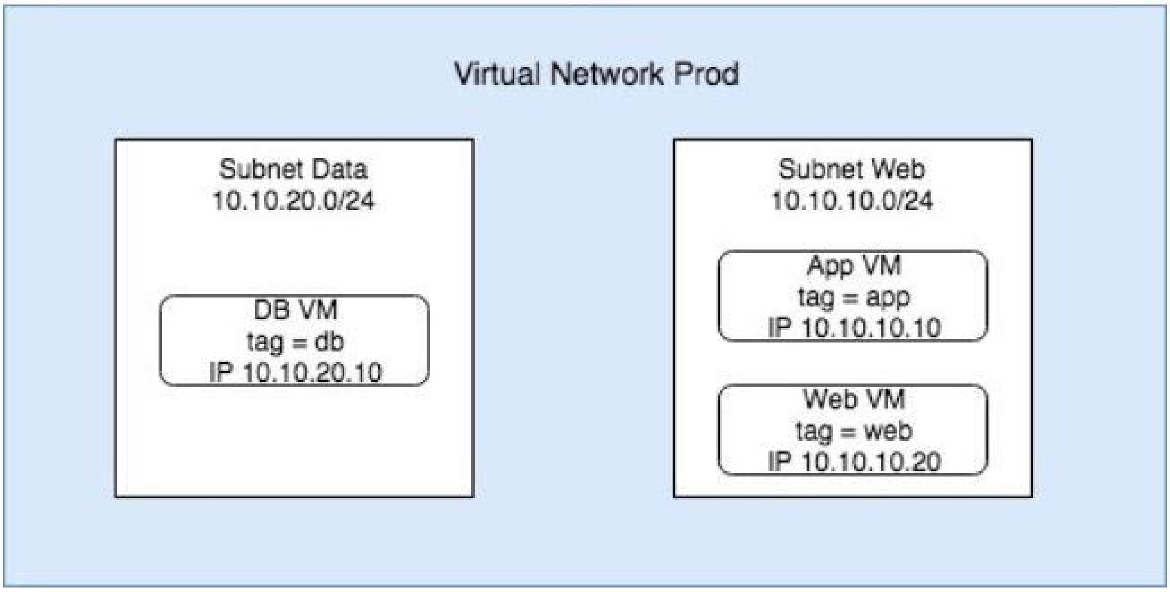
18. You have implemented an HTTP(S) load balancer to balance requests across Compute Engine Virtual Machine instances. During peak times, your backend instances cannot handle the number of requests per second, which causes some requests to be dropped. Following Google-recommended practices, you want to efficiently scale the instances to avoid this scenario in the future. What should you do?

A. Use unmanaged instance groups, and upgrade the instance machine type to use a higher-performing CPU.
B. Use unmanaged instance groups, and double the number of instances you need at off-peak times.
C. Use managed instance groups, and turn on autoscaling based on the average CPU utilization of your instances.
D. Use managed instance groups, turn on autoscaling for HTTP(S) load balancing usage, and set target load balancing usage as a percentage of the serving rate.

19. Your application development team is beta-testing a new application over Dedicated Interconnect. This application uses a single TCP socket and requires 7-Gbps bandwidth for optimal performance. The development team notices that connectivity speed of the application is capped at 3 Gbps over Dedicated Interconnect. You want to resolve this problem. What should you do?

A. Order a new Interconnect to increase bandwidth.
B. Create a Cloud VPN in addition to the Interconnect, and ECMP traffic over both.
C. Instruct the development team to distribute their application traffic over multiple TCP flow sessions.
D. Instruct the development team to tune their application TCP congestion window, receive window, and all other tcp buffers.

20. You create a VPC named Prod in custom mode with two subnets, as shown below. You want to make sure that:
1) Only App VM can access the DB VM instance,
2) Web VM can access App VM,
3) Users outside the VPC can send HTTPS requests to Web VM only. Which two firewall rules should you create?



A. Block all traffic from source tag “web”.
B. Allow traffic from source tag “app” to port 80 only.
C. Allow all traffic from source tag “app” to target tag “db”.
D. Allow ingress traffic from 0.0.0.0/0 on port 80 and 443 for target tag “web”.
E. Allow ingress traffic using source filter = IP ranges where source IP ranges = 10.10.10.0/24.

Hint
Answers: C is correct because this rule will allow traffic from app VM to db VM.
Answers: D is correct because this will allow outside users to send request to web VM.
https://cloud.google.com/vpc/docs/using-flow-logs

21. You have implemented an HTTP(S) load balancer to balance requests across Compute Engine Virtual Machine instances. During peak times, your backend instances cannot handle the number of requests per second, which causes some requests to be dropped. Following Google-recommended practices, you want to efficiently scale the instances to avoid this scenario in the future. What should you do?

A. Use unmanaged instance groups, and upgrade the instance machine type to use a higher-performing CPU.
B. Use unmanaged instance groups, and double the number of instances you need at off-peak times.
C. Use managed instance groups, and turn on autoscaling based on the average CPU utilization of your instances.
D. Use managed instance groups, turn on autoscaling for HTTP(S) load balancing usage, and set target load balancing usage as a percentage of the serving rate.

Hint

Answers: D is correct because the autoscaling method leverages the load balancer and efficiently scales the instances.
https://cloud.google.com/compute/docs/autoscaler/scaling-cpu-load-balancing