Google

Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer

NEW QUESTION 1
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: A

Explanation:
A Shared VPC Admin can define a Security Admin by granting an IAM member the Security Admin (compute.securityAdmin) role to the host project. Security Admins manage firewall rules and SSL certificates.

NEW QUESTION 2
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 resolve
B. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google's public DNS 8.8.8.8.
C. Configure both an inbound server policy and outbound DNS forwarding zones with the target as the on-premises DNS resolve
D. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google Cloud's DNS resolver.
E. Configure an outbound DNS server policy, and set your alternative name server to be your on-premises DNS resolve
F. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google Cloud's DNS resolver.
G. Configure Cloud DNS to DNS peer with your on-premises DNS resolve
H. Configure your on-premises DNS resolver to forward Google Cloud zone queries to Google's public DNS 8.8.8.8.

Answer: A

NEW QUESTION 3
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 <interconnect>.
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: DE

Explanation:
https://cloud.google.com/network-connectivity/docs/interconnect/how-to/dedicated/retrieving-loas

NEW QUESTION 4
You converted an auto mode VPC network to custom mode. Since the conversion, some of your Cloud Deployment Manager templates are no longer working.
You want to resolve the problem.
What should you do?

A. Apply an additional IAM role to the Google API's service account to allow custom mode networks.
B. Update the VPC firewall to allow the Cloud Deployment Manager to access the custom mode networks.
C. Explicitly reference the custom mode networks in the Cloud Armor whitelist.
D. Explicitly reference the custom mode networks in the Deployment Manager templates.

Answer: D

NEW QUESTION 5
Your organization has Compute Engine instances in us-east1, us-west2, and us-central1. Your organization also has an existing Cloud Interconnect physical connection in the East Coast of the United States with a single VLAN attachment and Cloud Router in us-east1. You need to provide a design with high availability and ensure that if a region goes down, you still have access to all your other Virtual Private Cloud (VPC) subnets. You need to accomplish this in the most cost-effective manner possible. What should you do?

A. Configure your VPC routing in regional mode.Add an additional Cloud Interconnect VLAN attachment in the us-east1 region, and configure a Cloud Router in us-east1.
B. Configure your VPC routing in global mode.Add an additional Cloud Interconnect VLAN attachment in the us-east1 region, and configure a Cloud Router in us-east1.
C. Configure your VPC routing in global mode.Add an additional Cloud Interconnect VLAN attachment in the us-west2 region, and configure a Cloud Router in us-west2.
D. Configure your VPC routing in regional mode.Add additional Cloud Interconnect VLAN attachments in the us-west2 and us-central1 regions, and configure Cloud Routers in us-west2 and us-central1.

Answer: B

NEW QUESTION 6
You have an application running on Compute Engine that uses BigQuery to generate some results that are stored in Cloud Storage. You want to ensure that none of the application instances have external IP addresses.
Which two methods can you use to accomplish this? (Choose two.)

A. Enable Private Google Access on all the subnets.
B. Enable Private Google Access on the VPC.
C. Enable Private Services Access on the VPC.
D. Create network peering between your VPC and BigQuery.
E. Create a Cloud NAT, and route the application traffic via NAT gateway.

Answer: AE

Explanation:
https://cloud.google.com/nat/docs/overview#interaction-pga Specifications https://cloud.google.com/vpc/docs/configure-private-google-access#specifications

NEW QUESTION 7
You recently noticed a recurring daily spike in network usage in your Google Cloud project. You need to identify the virtual machine (VM) instances and type of traffic causing the spike in traffic utilization while minimizing the cost and management overhead required. What should you do?

A. Enable VPC Flow Logs and send the output to BigQuery for analysis.
B. Enable Firewall Rules Logging for all allowed traffic and send the output to BigQuery for analysis.
C. Configure Packet Mirroring to send all traffic to a V
D. Use Wireshark on the VM to identity traffic utilization for each VM in the VPC.
E. Deploy a third-party network appliance and configure it as the default gatewa
F. Use the third-party network appliance to identify users with high network traffic.

Answer: C

NEW QUESTION 8
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.)

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: AB

NEW QUESTION 9
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 mod
B. Peer both the VPCs via network peering.
C. Create the Distribution VPC in custom mod
D. Use the CIDR range 10.0.0.0/9. Create the necessary subnets, and then peer them via network peering.
E. Create the Distribution VPC in custom mod
F. Use the CIDR range 10.128.0.0/9. Create the necessary subnets, and then peer them via network peering.
G. Rename the default VPC as "Distribution" and peer it via network peering.

Answer: B

Explanation:
https://cloud.google.com/vpc/docs/vpc#ip-ranges

NEW QUESTION 10
Your company has a Virtual Private Cloud (VPC) with two Dedicated Interconnect connections in two different regions: us-west1 and us-east1. Each Dedicated Interconnect connection is attached to a Cloud Router in its respective region by a VLAN attachment. You need to configure a high availability failover path. By default, all ingress traffic from the on-premises environment should flow to the VPC using the us-west1 connection. If us-west1 is unavailable, you want traffic to be rerouted to us-east1. How should you configure the multi-exit discriminator (MED) values to enable this failover path?

A. Use regional routin
B. Set the us-east1 Cloud Router to a base priority of 100, and set the us-west1 CloudRouter to a base priority of 1
C. Use global routin
D. Set the us-east1 Cloud Router to a base priority of 100, and set the us-west1 Cloud Router to a base priority of 1
E. Use regional routin
F. Set the us-east1 Cloud Router to a base priority of 1000, and set the us-west1 Cloud Router to a base priority of 1
G. Use global routin
H. Set the us-east1 Cloud Router to a base priority of 1000, and set the us-west1 Cloud Router to a base priority of 1

Answer: A

NEW QUESTION 10
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 thisinstance 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: B

NEW QUESTION 13
You need to configure the Border Gateway Protocol (BGP) session for a VPN tunnel you just created between two Google Cloud VPCs, 10.1.0.0/16 and 172.16.0.0/16. You have a Cloud Router (router-1) in the 10.1.0.0/16 network and a second Cloud Router (router-2) in the 172.16.0.0/16 network. Which configuration should you use for the BGP session?

A. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	169.254.0.254	169.254.0.254	65502
router-2	if-tunnel-b-to-a-if-0	169.254.0.254	169.254.0.254	65501

B. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	10.1.0.1	172.16.0.1	15052
router-2	if-tunnel-b-to-a-if-0	172.16.0.1	10.1.0.1	15501

C. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	169.254.20.1	169.254.20.2	65002
router-2	if-tunnel-b-to-a-if-0	169.254.20.2	169.254.20.1	65001

D. C:\Users\Admin\Desktop\Data\Odt data\Untitled.jpg

Router	BGP Interface Name	BGP IP	BGP Peer IP	Peer ASN
router-1	if-tunnel-a-to-b-if-0	172.16.0.254	10.1.0.254	16552
router-2	if-tunnel-b-to-a-if-0	10.1.0.254	172.16.0.254	16551

Answer: C

NEW QUESTION 15
You suspect that one of the virtual machines (VMs) in your default Virtual Private Cloud (VPC) is under a denial-of-service attack. You need to analyze the incoming traffic for the VM to understand where the traffic is coming from. What should you do?

A. Enable Data Access audit logs of the VP
B. Analyze the logs and get the source IP addresses from the subnetworks.get field.
C. Enable VPC Flow Logs for the subne
D. Analyze the logs and get the source IP addresses from the connection field.
E. Enable VPC Flow Logs for the VP
F. Analyze the logs and get the source IP addresses from the src_location field.
G. Enable Data Access audit logs of the subne
H. Analyze the logs and get the source IP addresses from the networks.get field.

Answer: B

NEW QUESTION 17
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 rule
E. Use network tags to isolate access between the departments.

Answer: C

Explanation:
https://cloud.google.com/vpc/docs/vpc-peering

NEW QUESTION 22
Your company is working with a partner to provide a solution for a customer. Both your company and the partner organization are using GCP. There are applications in the partner's network that need access to some resources in your company's VPC. There is no CIDR overlap between the VPCs.
Which two solutions can you implement to achieve the desired results without compromising the security? (Choose two.)

A. VPC peering
B. Shared VPC

C. Cloud VPN
D. Dedicated Interconnect
E. Cloud NAT

Answer: AC

Explanation:
Google Cloud VPC Network Peering allows internal IP address connectivity across two Virtual Private Cloud (VPC) networks regardless of whether they belong to the same project or the same organization.

NEW QUESTION 23
You have configured Cloud CDN using HTTP(S) load balancing as the origin for cacheable content. Compression is configured on the web servers, but responses served by Cloud CDN are not compressed.
What is the most likely cause of the problem?

A. You have not configured compression in Cloud CDN.
B. You have configured the web servers and Cloud CDN with different compression types.
C. The web servers behind the load balancer are configured with different compression types.
D. You have to configure the web servers to compress responses even if the request has a Via header.

Answer: D

Explanation:
If responses served by Cloud CDN are not compressed but should be, check that the web server software running on your instances is configured to compress responses. By default, some web server software will automatically disable compression for requests that include a Via header. The presence of a Via header indicates the request was forwarded by a proxy. HTTP proxies such as HTTP(S) load balancing add a Via header to each request as required by the HTTP specification. To enable compression, you may have to override your web server's default configuration to tell it to compress responses even if the request had a Via header.

NEW QUESTION 26
Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from your on-premises network using Cloud Interconnect. You must configure access only to Google APIs and services that are supported by VPC Service Controls through hybrid connectivity with a service level agreement (SLA) in place. What should you do?

A. Configure the existing Cloud Routers to advertise the Google API's public virtual IP addresses.
B. Use Private Google Access for on-premises hosts with restricted.googleapis.com virtual IP addresses.
C. Configure the existing Cloud Routers to advertise a default route, and use Cloud NAT to translate traffic from your on-premises network.
D. Add Direct Peering links, and use them for connectivity to Google APIs that use public virtual IP addresses.

Answer: B

NEW QUESTION 29
You need to give each member of your network operations team least-privilege access to create, modify, and delete Cloud Interconnect VLAN attachments. What should you do?

A. Assign each user the editor role.
B. Assign each user the compute.networkAdmin role.
C. Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get.
D. Give each user the following permissions only: compute.interconnectAttachments.create, compute.interconnectAttachments.get, compute.routers.create, compute.routers.get, compute.routers.update.

Answer: D

Explanation:
https://cloud.google.com/interconnect/docs/how-to/dedicated/creating-vlan-attachments

NEW QUESTION 34
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 have recently engaged a traffic-scrubbing service and want to restrict your origin to allow connections only from the traffic-scrubbing service. What should you do?

A. Create a Cloud Armor Security Policy that blocks all traffic except for the traffic-scrubbing service.
B. Create a VPC Firewall rule that blocks all traffic except for the traffic-scrubbing service.
C. Create a VPC Service Control Perimeter that blocks all traffic except for the traffic-scrubbing service.
D. Create IPTables firewall rules that block all traffic except for the traffic-scrubbing service.

Answer: A

Explanation:
Global load balancer will proxy the connection . thus no trace of session origin IP. you should use Cloud Armor to geofence your service.
https://cloud.google.com/load-balancing/docs/https

NEW QUESTION 36
You need to establish network connectivity between three Virtual Private Cloud networks, Sales, Marketing, and Finance, so that users can access resources in all three VPCs. You configure VPC peering between the Sales VPC and the Finance VPC. You also configure VPC peering between the Marketing VPC and the Finance VPC. After you complete the configuration, some users cannot connect to resources in the Sales VPC and the Marketing VPC. You want to resolve the problem.

What should you do?

A. Configure VPC peering in a full mesh.
B. Alter the routing table to resolve the asymmetric route.
C. Create network tags to allow connectivity between all three VPCs.
D. Delete the legacy network and recreate it to allow transitive peering.

Answer: A

Explanation:
https://cloud.google.com/vpc/docs/using-vpc-peering

NEW QUESTION 38
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: C

Explanation:
https://cloud.google.com/load-balancing/docs/load-balancing-overview mentions to use global load balancer for IPv6 termination.

NEW QUESTION 42
You have an HA VPN connection with two tunnels running in active/passive mode between your Virtual Private Cloud (VPC) and on-premises network. Traffic over the connection has recently increased from 1 gigabit per second (Gbps) to 4 Gbps, and you notice that packets are being dropped. You need to configure your VPN connection to Google Cloud to support 4 Gbps. What should you do?

A. Configure the remote autonomous system number (ASN) to 4096.
B. Configure a second Cloud Router to scale bandwidth in and out of the VPC.
C. Configure the maximum transmission unit (MTU) to its highest supported value.
D. Configure a second set of active/passive VPN tunnels.

Answer: D

NEW QUESTION 46
You configured Cloud VPN with dynamic routing via Border Gateway Protocol (BGP). You added a custom route to advertise a network that is reachable over the VPN tunnel. However, the on-premises clients still cannot reach the network over the VPN tunnel. You need to examine the logs in Cloud Logging to confirm that the appropriate routers are being advertised over the VPN tunnel. Which filter should you use in Cloud Logging to examine the logs?

A. resource.type= “gce_router”
B. resource.type= “gce_network_region”
C. resource.type= “vpn_tunnel”
D. resource.type= “vpn_gateway”

Answer: C

NEW QUESTION 51
In order to provide subnet level isolation, you want to force instance-A in one subnet to route through a security appliance, called instance-B, in another subnet. What should you do?

A. Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with no tag.
B. Create a more specific route than the system-generated subnet route, pointing the next hop to instance-B with a tag applied to instance-A.
C. Delete the system-generated subnet route and create a specific route to instance-B with a tag applied to instance-A.
D. Move instance-B to another VPC and, using multi-NIC, connect instance-B's interface to instance-A's networ
E. Configure the appropriate routes to force traffic through to instance-A.

Answer: B

NEW QUESTION 53
You are planning a large application deployment in Google Cloud that includes on-premises connectivity. The application requires direct connectivity between workloads in all regions and on-premises locations without address translation, but all RFC 1918 ranges are already in use in the on-premises locations. What should you do?

A. Use multiple VPC networks with a transit network using VPC Network Peering.
B. Use overlapping RFC 1918 ranges with multiple isolated VPC networks.
C. Use overlapping RFC 1918 ranges with multiple isolated VPC networks and Cloud NAT.
D. Use non-RFC 1918 ranges with a single global VPC.

Answer: D

NEW QUESTION 58
Your organization has a new security policy that requires you to monitor all egress traffic payloads from your virtual machines in region us-west2. You deployed an intrusion detection system (IDS) virtual appliance in the same region to meet the new policy. You now need to integrate the IDS into the environment to monitor all

egress traffic payloads from us-west2. What should you do?

A. Enable firewall logging, and forward all filtered egress firewall logs to the IDS.
B. Enable VPC Flow Log
C. Create a sink in Cloud Logging to send filtered egress VPC Flow Logs to the IDS.
D. Create an internal TCP/UDP load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.
E. Create an internal HTTP(S) load balancer for Packet Mirroring, and add a packet mirroring policy filter for egress traffic.

Answer: B

NEW QUESTION 60
You need to define an address plan for a future new GKE cluster in your VPC. This will be a VPC native cluster, and the default Pod IP range allocation will be used. You must pre-provision all the needed VPC subnets and their respective IP address ranges before cluster creation. The cluster will initially have a single node, but it will be scaled to a maximum of three nodes if necessary. You want to allocate the minimum number of Pod IP addresses.
Which subnet mask should you use for the Pod IP address range?

A. /21
B. /22
C. /23
D. /25

Answer: B

Explanation:
https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips#cluster_sizing_secondary_range_pods

NEW QUESTION 65
You are configuring an HA VPN connection between your Virtual Private Cloud (VPC) and on-premises network. The VPN gateway is named VPN_GATEWAY_1. You need to restrict VPN tunnels created in the project to only connect to your on-premises VPN public IP address: 203.0.113.1/32. What should you do?

A. Configure a firewall rule accepting 203.0.113.1/32, and set a target tag equal to VPN_GATEWAY_1.
B. Configure the Resource Manager constraint constraints/compute.restrictVpnPeerIPs to use an allowList consisting of only the 203.0.113.1/32 address.
C. Configure a Google Cloud Armor security policy, and create a policy rule to allow 203.0.113.1/32.
D. Configure an access control list on the peer VPN gateway to deny all traffic except 203.0.113.1/32, and attach it to the primary external interface.

Answer: B

NEW QUESTION 69
You are designing a Partner Interconnect hybrid cloud connectivity solution with geo-redundancy across two metropolitan areas. You want to follow Google-recommended practices to set up the following region/metro pairs:
(region 1/metro 1)
(region 2/metro 2) What should you do?

A. Create a Cloud Router in region 1 with two VLAN attachments connected to metro1-zone1-x.Create a Cloud Router in region 2 with two VLAN attachments connected to metro1-zone2-x.
B. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone1-x.Create a Cloud Router in region 2 with two VLAN attachments connected to metro2-zone2-x.
C. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone2-x.Create a Cloud Router in region 2 with one VLAN attachment connected to metro2-zone2-x.
D. Create a Cloud Router in region 1 with one VLAN attachment connected to metro1-zone1-x and one VLAN attachment connected to metro1-zone2-x.Create a Cloud Router in region 2 with one VLAN attachment connected to metro2-zone1-x and one VLAN attachment to metro2-zone2-x.

Answer: B

NEW QUESTION 73
You are adding steps to a working automation that uses a service account to authenticate. You need to drive the automation the ability to retrieve files from a Cloud Storage bucket. Your organization requires using the least privilege possible.
What should you do?

A. Grant the compute.instanceAdmin to your user account.
B. Grant the iam.serviceAccountUser to your user account.
C. Grant the read-only privilege to the service account for the Cloud Storage bucket.
D. Grant the cloud-platform privilege to the service account for the Cloud Storage bucket.

Answer: C

NEW QUESTION 76
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.

Answer: DE

NEW QUESTION 77
Your company has separate Virtual Private Cloud (VPC) networks in a single region for two departments: Sales and Finance. The Sales department's VPC network already has connectivity to on-premises locations using HA VPN, and you have confirmed that the subnet ranges do not overlap. You plan to peer both VPC networks to use the same HA tunnels for on-premises connectivity, while providing internet connectivity for the Google Cloud workloads through Cloud NAT. Internet access from the on-premises locations should not flow through Google Cloud. You need to propagate all routes between the Finance department and on-premises locations. What should you do?

A. Peer the two VPCs, and use the default configuration for the Cloud Routers.
B. Peer the two VPCs, and use Cloud Router’s custom route advertisements to announce the peered VPC network ranges to the on-premises locations.
C. Peer the two VPC
D. Configure VPC Network Peering to export custom routes from Sales and import custom routes on Finance's VPC networ
E. Use Cloud Router’s custom route advertisements to announce a default route to the on-premises locations.
F. Peer the two VPC
G. Configure VPC Network Peering to export custom routes from Sales and import custom routes on Finance's VPC networ
H. Use Cloud Router’s custom route advertisements to announce the peered VPC network ranges to the on-premises locations.

Answer: A

NEW QUESTION 82
You have deployed an HTTP(s) load balancer, but health checks to port 80 on the Compute Engine virtual machine instance are failing, and no traffic is sent to your instances. You want to resolve the problem. Which commands should you run?

A. gcloud compute instances add-access-config instance-1
B. gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --destination-ranges 130.211.0.0/22,35.191.0.0/16 --direction EGRESS
C. gcloud compute firewall-rules create allow-lb --network load-balancer --allow tcp --source-ranges 130.211.0.0/22,35.191.0.0/16 --direction INGRESS
D. gcloud compute health-checks update http health-check --unhealthy-threshold 10

Answer: A

NEW QUESTION 83
You have an application hosted on a Compute Engine virtual machine instance that cannot communicate with a resource outside of its subnet. When you review the flow and firewall logs, you do not see any denied traffic listed.
During troubleshooting you find:
• Flow logs are enabled for the VPC subnet, and all firewall rules are set to log.
• The subnetwork logs are not excluded from Stackdriver.
• The instance that is hosting the application can communicate outside the subnet.
• Other instances within the subnet can communicate outside the subnet.
• The external resource initiates communication. What is the most likely cause of the missing log lines?

A. The traffic is matching the expected ingress rule.
B. The traffic is matching the expected egress rule.
C. The traffic is not matching the expected ingress rule.
D. The traffic is not matching the expected egress rule.

Answer: C

NEW QUESTION 88
You are designing the network architecture for your organization. Your organization has three developer teams: Web, App, and Database. All of the developer teams require access to Compute Engine instances to perform their critical tasks. You are part of a small network and security team that needs to provide network access to the developers. You need to maintain centralized control over network resources, including subnets, routes, and firewalls. You want to minimize operational overhead. How should you design this topology?

A. Configure a host project with a Shared VP
B. Create service projects for Web, App, and Database.
C. Configure one VPC for Web, one VPC for App, and one VPC for Databas
D. Configure HA VPN between each VPC.
E. Configure three Shared VPC host projects, each with a service project: one for Web, one for App, and one for Database.
F. Configure one VPC for Web, one VPC for App, and one VPC for Databas
G. Use VPC Network Peering to connect all VPCs in a full mesh.

Answer: C

NEW QUESTION 91
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?

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

NEW QUESTION 94
You are developing an HTTP API hosted on a Compute Engine virtual machine instance that must be invoked only by multiple clients within the same Virtual Private Cloud (VPC). You want clients to be able to get the IP address of the service. What should you do?

A. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwarding rul
B. Clients should use this IP address to connect to the service.
C. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url https://[INSTANCE_NAME].[ZONE].c.[PROJECT_ID].internal/.
D. Reserve a static external IP address and assign it to an HTTP(S) load balancing service's forwardingrul
E. Then, define an A record in Cloud DN
F. Clients should use the name of the A record to connect to the service.
G. Ensure that clients use Compute Engine internal DNS by connecting to the instance name with the url https://[API_NAME]/[API_VERSION]/.

Answer: C

NEW QUESTION 95
You are increasing your usage of Cloud VPN between on-premises and GCP, and you want to support more traffic than a single tunnel can handle. You want to increase the available bandwidth using Cloud VPN.
What should you do?

A. Double the MTU on your on-premises VPN gateway from 1460 bytes to 2920 bytes.
B. Create two VPN tunnels on the same Cloud VPN gateway that point to the same destination VPN gateway IP address.
C. Add a second on-premises VPN gateway with a different public IP addres
D. Create a second tunnel on the existing Cloud VPN gateway that forwards the same IP range, but points at the new on-premises gateway IP.
E. Add a second Cloud VPN gateway in a different region than the existing VPN gatewa
F. Create a new tunnel on the second Cloud VPN gateway that forwards the same IP range, but points to the existing on-premises VPN gateway IP address.

Answer: C

Explanation:
https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies#redundancy-options

NEW QUESTION 96
Your company's Google Cloud-deployed, streaming application supports multiple languages. The application development team has asked you how they should support splitting audio and video traffic to different backend Google Cloud storage buckets. They want to use URL maps and minimize operational overhead. They are currently using the following directory structure:
/fr/video
/en/video
/es/video
/../video
/fr/audio
/en/audio
/es/audio
/../audio
Which solution should you recommend?

A. Rearrange the directory structure, create a URL map and leverage a path rule such as /video/* and/audio/*.
B. Rearrange the directory structure, create DNS hostname entries for video and audio and leverage a path rule such as /video/* and /audio/*.
C. Leave the directory structure as-is, create a URL map and leverage a path rule such as \/[a-z]{2}\/video and \/[a-z]{2}\/audio.
D. Leave the directory structure as-is, create a URL map and leverage a path rule such as /*/video and /*/ audio.

Answer: A

Explanation:
https://cloud.google.com/load-balancing/docs/url-map#configuring_url_maps
Path matcher constraints Path matchers and path rules have the following constraints: A path rule can only include a wildcard character (*) after a forward slash character (/). For example, /videos/* and /videos/hd/* are valid for path rules, but /videos* and /videos/hd* are not. Path rules do not use regular expression or substring matching. For example, path rules for either /videos/hd or /videos/hd/* do not apply to a URL with the path /video/hd-abcd. However, a path rule for /video/* does apply to that path. https://cloud.google.com/load-balancing/docs/url-map-concepts#pm-constraints

NEW QUESTION 98
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: D

Explanation:
https://cloud.google.com/network-connectivity/docs/router/support/troubleshooting#ecmp

NEW QUESTION 100
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

Professional-Cloud-Network-Engineer Practice Exam Features:

* Professional-Cloud-Network-Engineer Questions and Answers Updated Frequently

* Professional-Cloud-Network-Engineer Practice Questions Verified by Expert Senior Certified Staff

* Professional-Cloud-Network-Engineer Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* Professional-Cloud-Network-Engineer Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year