

# Google

## Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer



**NEW QUESTION 1**

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:** BC

**Explanation:**

<https://cloud.google.com/dns/docs/best-practices>

**NEW QUESTION 2**

You need to define an address plan for a future new Google Kubernetes Engine (GKE) cluster in your Virtual Private Cloud (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:** A

**NEW QUESTION 3**

You are responsible for configuring firewall policies for your company in Google Cloud. Your security team has a strict set of requirements that must be met to configure firewall rules.

Always allow Secure Shell (SSH) from your corporate IP address. Restrict SSH access from all other IP addresses.

There are multiple projects and VPCs in your Google Cloud organization. You need to ensure that other VPC firewall rules cannot bypass the security team's requirements. What should you do?

- A. Configure a hierarchical firewall policy to the organization node to allow TCP port 22 for your corporate IP address with priority 0. Configure a hierarchical firewall policy to the organization node to deny TCP port 22 for all IP addresses with priority 1.
- B. Configure a VPC firewall rule to allow TCP port 22 for your corporate IP address with priority 0. Configure a VPC firewall rule to deny TCP port 22 for all IP addresses with priority 1.
- C. Configure a VPC firewall rule to allow TCP port 22 for your corporate IP address with priority 1. Configure a VPC firewall rule to deny TCP port 22 for all IP addresses with priority 0.
- D. Configure a hierarchical firewall policy to the organization node to allow TCP port 22 for your corporate IP address with priority 1. Configure a hierarchical firewall policy to the organization node to deny TCP port 22 for all IP addresses with priority 0.

**Answer:** A

**NEW QUESTION 4**

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 5**

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 6**

You are designing a new global application using Compute Engine instances that will be exposed by a global HTTP(S) load balancer. You need to secure your application from distributed denial-of-service and application layer (layer 7) attacks. What should you do?

- A. Configure VPC Service Controls and create a secure perimeter.
- B. Define fine-grained perimeter controls and enforce that security posture across your Google Cloud services and projects.
- C. Configure a Google Cloud Armor security policy in your project, and attach it to the backend service to secure the application.
- D. Configure VPC firewall rules to protect the Compute Engine instances against distributed denial-of-service attacks.
- E. Configure hierarchical firewall rules for the global HTTP(S) load balancer public IP address at the organization level.

**Answer:** C

**NEW QUESTION 7**

You are maintaining a Shared VPC in a host project. Several departments within your company have infrastructure in different service projects attached to the Shared VPC and use Identity and Access Management (IAM) permissions to manage the cloud resources in those projects. VPC Network Peering is also set up between the Shared VPC and a common services VPC that is not in a service project. Several users are experiencing failed connectivity between certain instances in different Shared VPC service projects and between certain instances and the internet. You need to validate the network configuration to identify whether a misconfiguration is the root cause of the problem. What should you do?

- A. Review the VPC audit logs in Cloud Logging for the affected instances.
- B. Use Secure Shell (SSH) to connect to the affected Compute Engine instances, and run a series of PING tests to the other affected endpoints and the 8.8.8.8 IPv4 address.
- C. Run Connectivity Tests from Network Intelligence Center to check connectivity between the affected endpoints in your network and the internet.
- D. Enable VPC Flow Logs for all VPCs, and review the logs in Cloud Logging for the affected instances.

**Answer:** C

**NEW QUESTION 8**

You recently deployed Compute Engine instances in regions us-west1 and us-east1 in a Virtual Private Cloud (VPC) with default routing configurations. Your company security policy mandates that virtual machines (VMs) must not have public IP addresses attached to them. You need to allow your instances to fetch updates from the internet while preventing external access. What should you do?

- A. Create a Cloud NAT gateway and Cloud Router in both us-west1 and us-east1.
- B. Create a single global Cloud NAT gateway and global Cloud Router in the VPC.
- C. Change the instances' network interface external IP address from None to Ephemeral.
- D. Create a firewall rule that allows egress to destination 0.0.0.0/0.

**Answer:** A

**NEW QUESTION 9**

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:** C

**Explanation:**

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

**NEW QUESTION 10**

You work for a university that is migrating to Google Cloud.

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 Dedicated Interconnect in the host project.
- B. Use Shared VPC, and deploy the VLAN attachments in the service project

- C. Connect the VLAN attachment to the Shared VPC's host project.
- D. Use standalone projects, and deploy the VLAN attachments in the individual project
- E. Connect the VLAN attachment to the standalone projects' Dedicated Interconnects.
- F. Use standalone projects and deploy the VLAN attachments and Dedicated Interconnects in each of the individual projects.

**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 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:** B

#### NEW QUESTION 13

You created a new VPC for your development team. You want to allow access to the resources in this VPC via SSH only. How should you configure your firewall rules?

- A. Create two firewall rules: one to block all traffic with priority 0, and another to allow port 22 with priority 1000.
- B. Create two firewall rules: one to block all traffic with priority 65536, and another to allow port 3389 with priority 1000.
- C. Create a single firewall rule to allow port 22 with priority 1000.
- D. Create a single firewall rule to allow port 3389 with priority 1000.

**Answer:** C

#### NEW QUESTION 18

Your company has just launched a new critical revenue-generating web application. You deployed the application for scalability using managed instance groups, autoscaling, and a network load balancer as frontend. One day, you notice severe bursty traffic that the caused autoscaling to reach the maximum number of instances, and users of your application cannot complete transactions. After an investigation, you think it as a DDOS attack. You want to quickly restore user access to your application and allow successful transactions while minimizing cost. Which two steps should you take? (Choose two.)

- A. Use Cloud Armor to blacklist the attacker's IP addresses.
- B. Increase the maximum autoscaling backend to accommodate the severe bursty traffic.
- C. Create a global HTTP(s) load balancer and move your application backend to this load balancer.
- D. Shut down the entire application in GCP for a few hour
- E. The attack will stop when the application is offline.
- F. SSH into the backend compute engine instances, and view the auth logs and syslogs to further understand the nature of the attack.

**Answer:** BE

#### NEW QUESTION 19

Your company has defined a resource hierarchy that includes a parent folder with subfolders for each department. Each department defines their respective project and VPC in the assigned folder and has the appropriate permissions to create Google Cloud firewall rules. The VPCs should not allow traffic to flow between them. You need to block all traffic from any source, including other VPCs, and delegate only the intra-VPC firewall rules to the respective departments. What should you do?

- A. Create a VPC firewall rule in each VPC to block traffic from any source, with priority 0.
- B. Create a VPC firewall rule in each VPC to block traffic from any source, with priority 1000.
- C. Create two hierarchical firewall policies per department's folder with two rules in each: a high-priority rule that matches traffic from the private CIDRs assigned to the respective VPC and sets the action to allow, and another lower-priority rule that blocks traffic from any other source.
- D. Create two hierarchical firewall policies per department's folder with two rules in each: a high-priority rule that matches traffic from the private CIDRs assigned to the respective VPC and sets the action to goto\_next, and another lower-priority rule that blocks traffic from any other source.

**Answer:** B

#### NEW QUESTION 20

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:** B

#### Explanation:

[https://cloud.google.com/armor/docs/security-policy-concepts#preview\\_mode](https://cloud.google.com/armor/docs/security-policy-concepts#preview_mode)

**NEW QUESTION 23**

You are configuring a new HTTP application that will be exposed externally behind both IPv4 and IPv6 virtual IP addresses, using ports 80, 8080, and 443. You will have backends in two regions: us-west1 and us-east1. You want to serve the content with the lowest-possible latency while ensuring high availability and autoscaling, and create native content-based rules using the HTTP hostname and request path. The IP addresses of the clients that connect to the load balancer need to be visible to the backends. Which configuration should you use?

- A. Use Network Load Balancing
- B. Use TCP Proxy Load Balancing with PROXY protocol enabled
- C. Use External HTTP(S) Load Balancing with URL Maps and custom headers
- D. Use External HTTP(S) Load Balancing with URL Maps and an X-Forwarded-For header

**Answer:** D

**NEW QUESTION 27**

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 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 33**

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.
- B. Enable Cloud CDN on the load balancers. Create an A record in Cloud DNS with both IP addresses for the load balancers.
- C. 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.
- D. 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.
- E. 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.
- F. Enable Cloud CDN on the load balancer. Create a CNAME record using the load balancer's IP address in Cloud DNS.

**Answer:** C

**NEW QUESTION 34**

You work for a multinational enterprise that is moving to GCP. These are the cloud requirements:

- An on-premises data center located in the United States in Oregon and New York with Dedicated Interconnects connected to Cloud regions us-west1 (primary HQ) and us-east4 (backup)
- Multiple regional offices in Europe and APAC
- Regional data processing is required in europe-west1 and australia-southeast1
- Centralized Network Administration Team

Your security and compliance team requires a virtual inline security appliance to perform L7 inspection for URL filtering. You want to deploy the appliance in us-west1.

What should you do?

- A. • Create 2 VPCs in a Shared VPC Host Project. • Configure a 2-NIC instance in zone us-west1-a in the Host Project. • Attach NIC0 in VPC #1 us-west1 subnet of the Host Project. • Attach NIC1 in VPC #2 us-west1 subnet of the Host Project. • Deploy the instance. • Configure the necessary routes and firewall rules to pass traffic through the instance.
- B. • Create 2 VPCs in a Shared VPC Host Project. • Configure a 2-NIC instance in zone us-west1-a in the Service Project. • Attach NIC0 in VPC #1 us-west1 subnet of the Host Project. • Attach NIC1 in VPC #2 us-west1 subnet of the Host Project. • Deploy the instance. • Configure the necessary routes and firewall rules

to pass traffic through the instance.

C. • Create 1 VPC in a Shared VPC Host Project. • Configure a 2-NIC instance in zone us-west1-a in the Host Project. • Attach NIC0 in us-west1 subnet of the Host Project. • Attach NIC1 in us-west1 subnet of the Host Project • Deploy the instance. • Configure the necessary routes and firewall rules to pass traffic through the instance.

D. • Create 1 VPC in a Shared VPC Service Project. • Configure a 2-NIC instance in zone us-west1-a in the Service Project. • Attach NIC0 in us-west1 subnet of the Service Project. • Attach NIC1 in us-west1 subnet of the Service Project • Deploy the instance. • Configure the necessary routes and firewall rules to pass traffic through the instance.

**Answer:** B

**Explanation:**

<https://cloud.google.com/vpc/docs/shared-vpc>

#### NEW QUESTION 35

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.

**Answer:** C

#### NEW QUESTION 38

You create multiple Compute Engine virtual machine instances to be used as TFTP servers. Which type of load balancer should you use?

- A. HTTP(S) load balancer
- B. SSL proxy load balancer
- C. TCP proxy load balancer
- D. Network load balancer

**Answer:** D

**Explanation:**

"TFTP is a UDP-based protocol. Servers listen on port 69 for the initial client-to-server packet to establish the TFTP session, then use a port above 1023 for all further packets during that session. Clients use ports above 1023" [https://docstore.mik.ua/orelly/networking\\_2ndEd/fire/ch17\\_02.htm](https://docstore.mik.ua/orelly/networking_2ndEd/fire/ch17_02.htm) Besides, Google Cloud external TCP/UDP Network Load Balancing (after this referred to as Network Load Balancing) is a regional, non-proxied load balancer. Network Load Balancing distributes traffic among virtual machine (VM) instances in the same region in a Virtual Private Cloud (VPC) netw

#### NEW QUESTION 42

You want to configure a NAT to perform address translation between your on-premises network blocks and GCP. Which NAT solution should you use?

- A. Cloud NAT
- B. An instance with IP forwarding enabled
- C. An instance configured with iptables DNAT rules
- D. An instance configured with iptables SNAT rules

**Answer:** A

#### NEW QUESTION 47

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 51

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

**NEW QUESTION 54**

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 59**

You need to configure a static route to an on-premises resource behind a Cloud VPN gateway that is configured for policy-based routing using the gcloud command.

Which next hop should you choose?

- A. The default internet gateway
- B. The IP address of the Cloud VPN gateway
- C. The name and region of the Cloud VPN tunnel
- D. The IP address of the instance on the remote side of the VPN tunnel

**Answer:** C

**Explanation:**

When you create a route based tunnel using the Cloud Console, Classic VPN performs both of the following tasks: Sets the tunnel's local and remote traffic selectors to any IP address (0.0.0.0/0) For each range in Remote network IP ranges, Google Cloud creates a custom static route whose destination (prefix) is the range's CIDR, and whose next hop is the tunnel.

<https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns>

**NEW QUESTION 64**

Your company has a single Virtual Private Cloud (VPC) network deployed in Google Cloud with access from on-premises locations using Cloud Interconnect connections. Your company must be able to send traffic to Cloud Storage only through the Interconnect links while accessing other Google APIs and services over the public internet. What should you do?

- A. Use the default public domains for all Google APIs and services.
- B. Use Private Service Connect to access Cloud Storage, and use the default public domains for all other Google APIs and services.
- C. Use Private Google Access, with restricted.googleapis.com virtual IP addresses for Cloud Storage and private.googleapis.com for all other Google APIs and services.
- D. Use Private Google Access, with private.googleapis.com virtual IP addresses for Cloud Storage and restricted.googleapis.com virtual IP addresses for all other Google APIs and services.

**Answer:** B

**NEW QUESTION 66**

You are the network administrator responsible for hybrid connectivity at your organization. Your developer team wants to use Cloud SQL in the us-west1 region in your Shared VPC. You configured a Dedicated Interconnect connection and a Cloud Router in us-west1, and the connectivity between your Shared VPC and on-premises data center is working as expected. You just created the private services access connection required for Cloud SQL using the reserved IP address range and default settings. However, your developers cannot access the Cloud SQL instance from on-premises. You want to resolve the issue. What should you do?

- A. Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes. Create a custom route advertisement in your Cloud Router to advertise the Cloud SQL IP address range.
- B. Change the VPC routing mode to global. Create a custom route advertisement in your Cloud Router to advertise the Cloud SQL IP address range.
- C. Create an additional Cloud Router in us-west2. Create a new Border Gateway Protocol (BGP) peering connection to your on-premises data center.
- D. Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes.
- E. Change the VPC routing mode to global. Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export of routes.

**Answer:** A

**NEW QUESTION 70**

Your company has recently expanded their EMEA-based operations into APAC. Globally distributed users report that their SMTP and IMAP services are slow. Your company requires end-to-end encryption, but you do not have access to the SSL certificates.

Which Google Cloud load balancer should you use?

- A. SSL proxy load balancer
- B. Network load balancer
- C. HTTPS load balancer
- D. TCP proxy load balancer

**Answer:** D

**Explanation:**

<https://cloud.google.com/security/encryption-in-transit/> Automatic encryption between GFEs and backends For the following load balancer types, Google automatically encrypts traffic between Google Front Ends (GFEs) and your backends that reside within Google Cloud VPC networks: HTTP(S) Load Balancing TCP Proxy Load Balancing SSL Proxy Load Balancing

**NEW QUESTION 75**

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 network
- 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 network
- H. Use Cloud Router's custom route advertisements to announce the peered VPC network ranges to the on-premises locations.

**Answer:** A

**NEW QUESTION 77**

Your software team is developing an on-premises web application that requires direct connectivity to Compute Engine Instances in GCP using the RFC 1918 address space. You want to choose a connectivity solution from your on-premises environment to GCP, given these specifications:

- Your ISP is a Google Partner Interconnect provider.
- Your on-premises VPN device's internet uplink and downlink speeds are 10 Gbps.
- A test VPN connection between your on-premises gateway and GCP is performing at a maximum speed of 500 Mbps due to packet losses.
- Most of the data transfer will be from GCP to the on-premises environment.
- The application can burst up to 1.5 Gbps during peak transfers over the Interconnect.
- Cost and the complexity of the solution should be minimal.

How should you provision the connectivity solution?

- A. Provision a Partner Interconnect through your ISP.
- B. Provision a Dedicated Interconnect instead of a VPN.
- C. Create multiple VPN tunnels to account for the packet losses, and increase bandwidth using ECMP.
- D. Use network compression over your VPN to increase the amount of data you can send over your VPN.

**Answer:** A

**Explanation:**

Direct Interconnect will be too expensive and also an overkill for this requirement. Managing multiple tunnels that too with packet loss consideration is complex also. Whereas partner interconnect fits the bill with providing required bandwidth but not super expensive also once setup not too complex too manage.

**NEW QUESTION 79**

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 80**

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 address
- 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 gateway
- 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 85**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The Professional-Cloud-Network-Engineer Practice Test Here](#)**