Exam Questions Professional-Cloud-Network-Engineer

Google Cloud Certified - Professional Cloud Network Engineer

https://www.2passeasy.com/dumps/Professional-Cloud-Network-Engineer/

NEW QUESTION 1
You built a web application with several containerized microservices. You want to run those microservices on Cloud Run. You must also ensure that the services are highly available to your customers with low latency. What should you do?

A. Deploy the Cloud Run services to multiple availability zone
B. Create a global TCP load balance
C. Addthe Cloud Run endpoints to its backend service.
D. Deploy the Cloud Run services to multiple region
E. Create serverless network endpoint groups (NEGs) that point to the service
F. Create a global HTTPS load balancer, and attach the serverless NEGs as backend services of the load balancer.
G. Deploy the Cloud Run services to multiple availability zone
H. Create Cloud Endpoints that point to the service
I. Create a global HTTPS load balancer, and attach the Cloud Endpoints to its backend
J. Deploy the Cloud Run services to multiple region
K. Configure a round-robin A record in Cloud DNS.

Answer: B

NEW QUESTION 2
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 3
You have deployed a new internal application that provides HTTP and TFTP services to on-premises hosts. You want to be able to distribute traffic across multiple Compute Engine instances, but need to ensure that clients are sticky to a particular instance across both services.
Which session affinity should you choose?

A. None
B. Client IP
C. Client IP and protocol
D. Client IP, port and protocol

Answer: B

NEW QUESTION 4
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 1Configure a hierarchical firewall policy to the organization node to deny TCP port 22 for all IP addresses with priority 0.

Answer: A

NEW QUESTION 5
You need to enable Cloud CDN for all the objects inside a storage bucket. You want to ensure that all the object in the storage bucket can be served by the CDN. What should you do in the GCP Console?

A. Create a new cloud storage bucket, and then enable Cloud CDN on it.

B. Create a new TCP load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.
C. Create a new SSL proxy load balancer, select the storage bucket as a backend, and then enable Cloud CDN on the backend.
D. Create a new HTTP load balancer, select the storage bucket as a backend, enable Cloud CDN on the backend, and make sure each object inside the storage bucket is shared publicly.

Answer: D

Explanation:
https://cloud.google.com/load-balancing/docs/https/adding-backend-buckets-to-load-balancers#using_cloud_cdn Cloud CDN needs HTTP(S) Load Balancers and Cloud Storage bucket has to be shared publicly.
https://cloud.google.com/cdn/docs/setting-up-cdn-with-bucket

NEW QUESTION 6
You created a new VPC network named Dev with a single subnet. You added a firewall rule for the network Dev to allow HTTP traffic only and enabled logging. When you try to log in to an instance in the subnet via Remote Desktop Protocol, the login fails. You look for the Firewall rules logs in Stackdriver Logging, but you do not see any entries for blocked traffic. You want to see the logs for blocked traffic.
What should you do?

A. Check the VPC flow logs for the instance.
B. Try connecting to the instance via SSH, and check the logs.
C. Create a new firewall rule to allow traffic from port 22, and enable logs.
D. Create a new firewall rule with priority 65500 to deny all traffic, and enable logs.

Answer: D

Explanation:
Ingress packets in VPC Flow Logs are sampled after ingress firewall rules. If an ingress firewall rule denies inbound packets, those packets are not sampled by VPC Flow Logs. We want to see the logs for blocked traffic so we have to look for them in firewall logs.
https://cloud.google.com/vpc/docs/flow-logs#key_properties

NEW QUESTION 7
You have enabled HTTP(S) load balancing for your application, and your application developers have reported that HTTP(S) requests are not being distributed correctly to your Compute Engine Virtual Machine instances. You want to find data about how the request are being distributed.
Which two methods can accomplish this? (Choose two.)

A. On the Load Balancer details page of the GCP Console, click on the Monitoring tab, select your backend service, and look at the graphs.
B. In Stackdriver Error Reporting, look for any unacknowledged errors for the Cloud Load Balancers service.
C. In Stackdriver Monitoring, select Resources > Metrics Explorer and search for https/request_bytes_count metric.
D. In Stackdriver Monitoring, select Resources > Google Cloud Load Balancers and review the Key Metrics graphs in the dashboard.
E. In Stackdriver Monitoring, create a new dashboard and track the https/backend_request_count metric for the load balancer.

Answer: AE

NEW QUESTION 8
You need to enable Private Google Access for use by some subnets within your Virtual Private Cloud (VPC). Your security team set up the VPC to send all internet-bound traffic back to the on- premises data center for inspection before egressing to the internet, and is also implementing VPC Service Controls in the environment for API-level security control. You have already enabled the subnets for Private Google Access. What configuration changes should you make to enable Private Google Access while adhering to your security team’s requirements?

A. Create a private DNS zone with a CNAME record for *.googleapis.com to restricted.googleapis.com, with an A record pointing to Google's restricted API address range.Create a custom route that points Google's restricted API address range to the default internet gateway as the next hop.
B. Create a private DNS zone with a CNAME record for *.googleapis.com to restricted.googleapis.com, with an A record pointing to Google's restricted API address range.Change the custom route that points the default route (0/0) to the default internet gateway as the next hop.
C. Create a private DNS zone with a CNAME record for *.googleapis.com to private.googleapis.com, with an A record painting to Google's private AP address range.Change the custom route that points the default route (0/0) to the default internet gateway as the next hop.
D. Create a private DNS zone with a CNAME record for *.googleapis.com to private.googleapis.com, with an A record pointing to Google's private API address range.Create a custom route that points Google's private API address range to the default internet gateway as the next hop.

Answer: C

NEW QUESTION 9
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 10

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 perimete
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 10
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 14
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 19
You have applications running in the us-west1 and us-east1 regions. You want to build a highly available VPN that provides 99.99% availability to connect your applications from your project to the cloud services provided by your partner's project while minimizing the amount of infrastructure required. Your partner's services are also in the us-west1 and us-east1 regions. You want to implement the simplest solution. What should you do?

A. Create one Cloud Router and one HA VPN gateway in each region of your VPC and your partner's VP
B. Connect your VPN gateways to the partner's gateway
C. Enable global dynamic routing in each VPC.
D. Create one Cloud Router and one HA VPN gateway in the us-west1 region of your VP
E. Create one OpenVPN Access Server in each region of your partner's VP
F. Connect your VPN gateway to your partner's servers.
G. Create one OpenVPN Access Server in each region of your VPC and your partner's VP
H. Connect your servers to the partner's servers.
I. Create one Cloud Router and one HA VPN gateway in the us-west1 region of your VPC and your partner's VP
J. Connect your VPN gateways to the partner's gateways with a pair of tunnel
K. Enable global dynamic routing in each VPC.

Answer: A

NEW QUESTION 22
You are designing a hybrid cloud environment for your organization. Your Google Cloud environment is interconnected with your on-premises network using Cloud HA VPN and Cloud Router. The Cloud Router is
configured with the default settings. Your on-premises DNS server is located at 192.168.20.88 and is protected by a firewall, and your Compute Engine resources are located at 10.204.0.0/24. Your Compute Engine resources need to resolve on-premises private hostnames using the domain corp.altostrat.com while still resolving Google Cloud hostnames. You want to follow Google-recommended practices. What should you do?

A. Create a private forwarding zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com that points to 192.168.20.88.Configure your on-premises firewall to accept traffic from 10.204.0.0/24. Set a custom route advertisement on the Cloud Router for 10.204.0.0/24
B. Create a private forwarding zone in Cloud DNS for ‘corp.altostrat.com’ called corp-altostrat-com that points to 192.168 20.88.Configure your on-premises firewall to accept traffic from 35.199.192.0/19 Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.
C. Create a private forwarding zone in Cloud DNS for ‘corp .altostrat.com’ called corp-altostrat-com that points to 192.168.20.88.Configure your on-premises firewall to accept traffic from 10.204.0.0/24.Modify the /etc/resolv conf file on your Compute Engine instances to point to 192.168.20 88
D. Create a private zone in Cloud DNS for ‘corp altostrat.com’ called corp-altostrat-com.Configure DNS Server Policies and create a policy with Alternate DNS

servers to 192.168.20.88. Configure your on-premises firewall to accept traffic from 35.199.192.0/19.Set a custom route advertisement on the Cloud Router for 35.199.192.0/19.

Answer: D

NEW QUESTION 23
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 25
You have provisioned a Partner Interconnect connection to extend connectivity from your on-premises data center to Google Cloud. You need to configure a Cloud Router and create a VLAN attachment to connect to resources inside your VPC. You need to configure an Autonomous System number (ASN) to use with the associated Cloud Router and create the VLAN attachment.
What should you do?

A. Use a 4-byte private ASN 4200000000-4294967294.
B. Use a 2-byte private ASN 64512-65535.
C. Use a public Google ASN 15169.
D. Use a public Google ASN 16550.

Answer: B

NEW QUESTION 29
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 33
Your on-premises data center has 2 routers connected to your GCP 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 the same 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.
•The VPN logs have no-proposal-chosen lines when the VPNs are connecting.
•BGP session is not established between one on-premises router and the Cloud Router. What is the most likely cause of this problem?

A. One of the VPN sessions is configured incorrectly.
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. BGP sessions are not established between both on-premises routers and the Cloud Router.

Answer: A

Explanation:
If the VPN logs show a no-proposal-chosen error, this error indicates that Cloud VPN and your peer VPN gateway were unable to agree on a set of ciphers. For IKEv1, the set of ciphers must match exactly. For IKEv2, there must be at least one common cipher proposed by each gateway. Make sure that you use supported ciphers to configure your peer VPN gateway.
https://cloud.google.com/network-connectivity/docs/vpn/support/troubleshooting#:~:text=If%20the%20VPN%2

NEW QUESTION 35
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 39
Your company is running out of network capacity to run a critical application in the on-premises data center. You want to migrate the application to GCP. You also want to ensure that the Security team does not lose their ability to monitor traffic to and from Compute Engine instances.
Which two products should you incorporate into the solution? (Choose two.)

A. VPC flow logs
B. Firewall logs
C. Cloud Audit logs
D. Stackdriver Trace
E. Compute Engine instance system logs

Answer: AB

Explanation:
A: Using VPC Flow Logs VPC Flow Logs records a sample of network flows sent from and received by VM instances, including instances used as GKE nodes. These logs can be used for network monitoring, forensics, real-time security analysis, and expense optimization. https://cloud.google.com/vpc/docs/using-flow-logs
(B): Firewall Rules Logging overview Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules. For example, you can determine if a firewall rule designed to deny traffic is functioning
as intended. Firewall Rules Logging is also useful if you need to determine how many connections are affected by a given firewall rule. You enable Firewall Rules Logging individually for each firewall rule whose connections you need to log. Firewall Rules Logging is an option for any firewall rule, regardless of the action (allow or deny) or direction (ingress or egress) of the rule.
https://cloud.google.com/vpc/docs/firewall-rules-logging

NEW QUESTION 44
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 45
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 48
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 50
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 52
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 54
After a network change window one of your company’s applications stops working. The application uses an on-premises database server that no longer receives any traffic from the application. The database server IP address is 10.2.1.25. You examine the change request, and the only change is that 3 additional VPC subnets were created. The new VPC subnets created are 10.1.0.0/16, 10.2.0.0/16, and 10.3.1.0/24/ The on-premises router is advertising 10.0.0.0/8.
What is the most likely cause of this problem?

A. The less specific VPC subnet route is taking priority.
B. The more specific VPC subnet route is taking priority.
C. The on-premises router is not advertising a route for the database server.
D. A cloud firewall rule that blocks traffic to the on-premises database server was created during the change.

Answer: B

NEW QUESTION 55
You decide to set up Cloud NAT. After completing the configuration, you find that one of your instances is not using the Cloud NAT for outbound NAT.
What is the most likely cause of this problem?

A. The instance has been configured with multiple interfaces.
B. An external IP address has been configured on the instance.
C. You have created static routes that use RFC1918 ranges.
D. The instance is accessible by a load balancer external IP address.

Answer: B

NEW QUESTION 60
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 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)

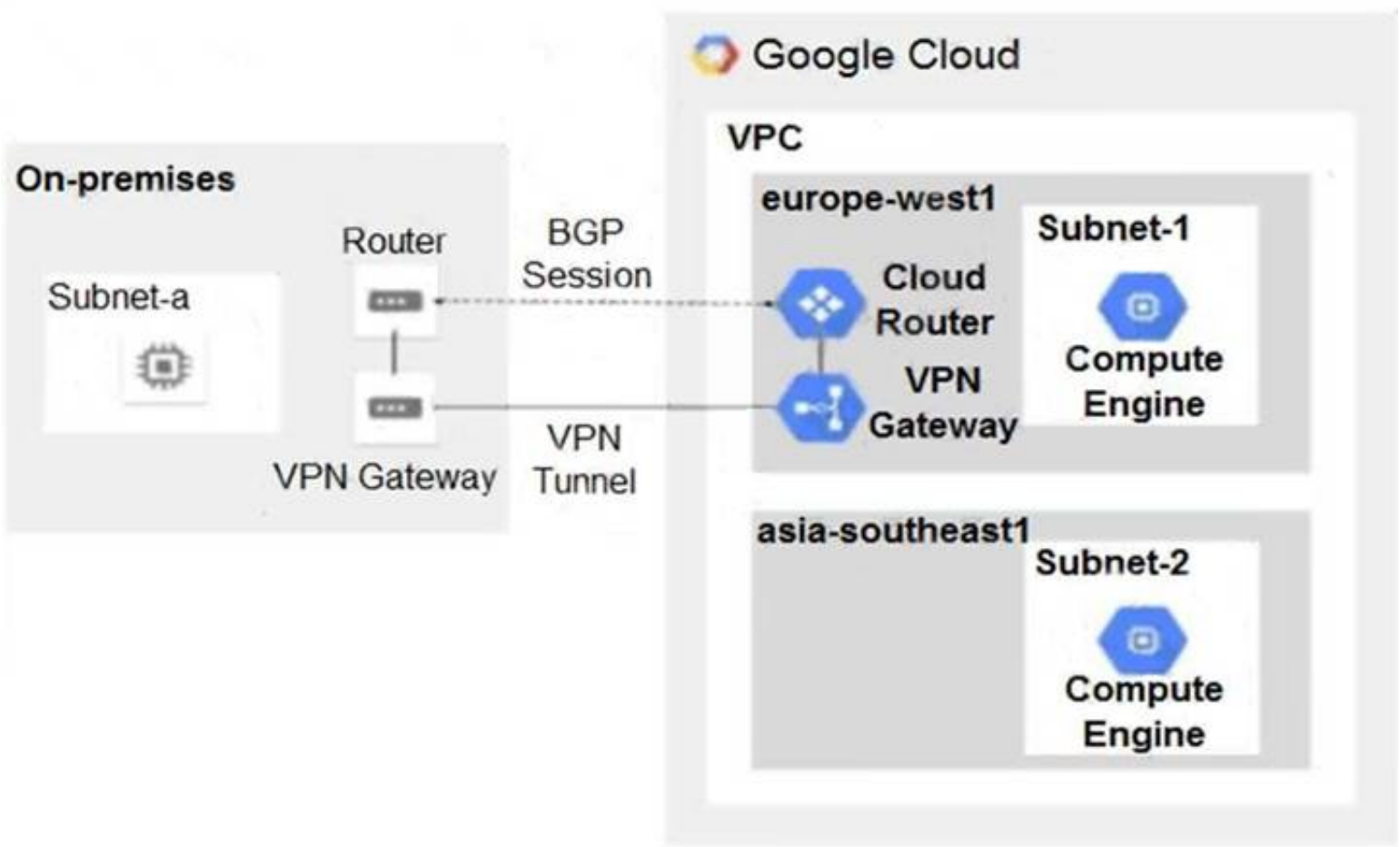
netw

NEW QUESTION 64
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 67
You have the following routing design. You discover that Compute Engine instances in Subnet-2 in the asia-southeast1 region cannot communicate with compute resources on-premises. What should you do?



A. Configure a custom route advertisement on the Cloud Router.
B. Enable IP forwarding in the asia-southeast1 region.
C. Change the VPC dynamic routing mode to Global.
D. Add a second Border Gateway Protocol (BGP) session to the Cloud Router.

Answer: C

NEW QUESTION 71
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 74
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 78
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 80
You successfully provisioned a single Dedicated Interconnect. The physical connection is at a colocation facility closest to us-west2. Seventy-five percent of your workloads are in us-east4, and the remaining twenty-five percent of your workloads are in us-central1. All workloads have the same network traffic profile. You need to minimize data transfer costs when deploying VLAN attachments. What should you do?

A. Keep the existing Dedicated interconnec
B. Deploy a VLAN attachment to a Cloud Router in us-west2, and use VPC global routing to access workloads in us-east4 and us-central1.
C. Keep the existing Dedicated Interconnec
D. Deploy a VLAN attachment to a Cloud Router in us-east4, and deploy another VLAN attachment to a Cloud Router in us-central1.
E. Order a new Dedicated Interconnect for a colocation facility closest to us-east4, and use VPC globalrouting to access workloads in us-central1.
F. Order a new Dedicated Interconnect for a colocation facility closest to us-central1, and use VPC global routing to access workloads in us-east4.

Answer: C

NEW QUESTION 85
Your organization uses a hub-and-spoke architecture with critical Compute Engine instances in your Virtual Private Clouds (VPCs). You are responsible for the design of Cloud DNS in Google Cloud. You need to be able to resolve Cloud DNS private zones from your on-premises data center and enable on-premises name resolution from your hub-and-spoke VPC design. What should you do?

A. Configure a private DNS zone in the hub VPC, and configure DNS forwarding to the on-premises server.Configure DNS peering from the spoke VPCs to the hub VPC.
B. Configure a DNS policy in the hub VPC to allow inbound query forwarding from the spoke VPCs.Configure the spoke VPCs with a private zone, and set up DNS peering to the hub VPC.
C. Configure a DNS policy in the spoke VPCs, and configure your on-premises DNS as an alternate DNS server.Configure the hub VPC with a private zone, and set up DNS peering to each of the spoke VPCs.
D. Configure a DNS policy in the hub VPC, and configure the on-premises DNS as an alternate DNS server.Configure the spoke VPCs with a private zone, and set up DNS peering to the hub VPC.

Answer: C

NEW QUESTION 89
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 93
You recently configured Google Cloud Armor security policies to manage traffic to your application. You discover that Google Cloud Armor is incorrectly blocking some traffic to your application. You need to identity the web application firewall (WAF) rule that is incorrectly blocking traffic. What should you do?

A. Enable firewall logs, and view the logs in Firewall Insights.
B. Enable HTTP(S) Load Balancing logging with sampling rate equal to 1, and view the logs in Cloud Logging.
C. Enable VPC Flow Logs, and view the logs in Cloud Logging.
D. Enable Google Cloud Armor audit logs, and view the logs on the Activity page in the Google CloudConsole.

Answer: A

NEW QUESTION 97
You are migrating a three-tier application architecture from on-premises to Google Cloud. As a first step in the migration, you want to create a new Virtual Private Cloud (VPC) with an external HTTP(S) load balancer. This load balancer will forward traffic back to the on-premises compute resources that run the presentation tier. You need to stop malicious traffic from entering your VPC and consuming resources at the edge, so you must configure this policy to filter IP addresses and stop cross-site scripting (XSS) attacks. What should you do?

A. Create a Google Cloud Armor policy, and apply it to a backend service that uses an unmanaged instance group backend.

B. Create a hierarchical firewall ruleset, and apply it to the VPC's parent organization resource node.
C. Create a Google Cloud Armor policy, and apply it to a backend service that uses an internet network endpoint group (NEG) backend.
D. Create a VPC firewall ruleset, and apply it to all instances in unmanaged instance groups.

Answer: C

NEW QUESTION 100
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 105
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 cente
D. Modify the VPC Network Peering connection used for Cloud SQL, and enable the import and export ofroutes.
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 108
You have the following firewall ruleset applied to all instances in your Virtual Private Cloud (VPC):

Direction	Action	Address range	Port	Priority
egress	deny	192.0.2.0/24	80	100
egress	deny	198.51.100.0/24	80	200
ingress	allow	203.0.113.0/24	80	300

You need to update the firewall rule to add the following rule to the ruleset:

Direction	Action	Address range	Port	Logging
egress	deny	192.0.2.42/32	80	true

You are using a new user account. You must assign the appropriate identity and Access Management (IAM) user roles to this new user account before updating the firewall rule. The new user account must be able to apply the update and view firewall logs. What should you do?

A. Assign the compute.securityAdmin and logging.viewer rule to the new user accoun
B. Apply the new firewall rule with a priority of 50.
C. Assign the compute.securityAdmin and logging.bucketWriter role to the new user accoun
D. Apply the new firewall rule with a priority of 150.
E. Assign the compute.orgSecurityPolicyAdmin and logging.viewer role to the new user accoun
F. Apply the new firewall rule with a priority of 50.
G. Assign the compute.orgSecurityPolicyAdmin and logging.bucketWriter role to the new user account.Apply the new firewall rule with a priority of 150.

Answer: A

NEW QUESTION 111
You have a storage bucket that contains two objects. Cloud CDN is enabled on the bucket, and both objects have been successfully cached. Now you want to make sure that one of the two objects will not be cached anymore, and will always be served to the internet directly from the origin.
What should you do?

A. Ensure that the object you don’t want to be cached anymore is not shared publicly.
B. Create a new storage bucket, and move the object you don’t want to be checked anymore inside i
C. Then edit the bucket setting and enable the private attribute.
D. Add an appropriate lifecycle rule on the storage bucket containing the two objects.
E. Add a Cache-Control entry with value private to the metadata of the object you don’t want to be cached anymor
F. Invalidate all the previously cached copies.

Answer: D

Explanation:
https://cloud.google.com/cdn/docs/invalidating-cached-content

NEW QUESTION 112
Your company has recently installed a Cloud VPN tunnel between your on-premises data center and your Google Cloud Virtual Private Cloud (VPC). You need to configure access to the Cloud Functions API for your on-premises servers. The configuration must meet the following requirements:
Certain data must stay in the project where it is stored and not be exfiltrated to other projects.
Traffic from servers in your data center with RFC 1918 addresses do not use the internet to access Google Cloud APIs.
All DNS resolution must be done on-premises.
The solution should only provide access to APIs that are compatible with VPC Service Controls. What should you do?

A. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range.Create a CNAME record for *.googleapis.com that points to the A record.Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.
B. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range.Create a CNAME record for *.googleapis.com that points to the A record.Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.Configure your on-premises firewalls to allow traffic to the restricted.googleapis.com addresses.
C. Create an A record for restricted.googleapis.com using the 199.36.153.4/30 address range.Create a CNAME record for *.googleapis.com that points to the A record.Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.Remove the default internet gateway from the VPC where your Cloud VPN tunnel terminates.
D. Create an A record for private.googleapis.com using the 199.36.153.8/30 address range.Create a CNAME record for *.googleapis.com that points to the A record.Configure your on-premises routers to use the Cloud VPN tunnel as the next hop for the addresses you used in the A record.Configure your on-premises firewalls to allow traffic to the private.googleapis.com addresses.

Answer: C

NEW QUESTION 113
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 114
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 115
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 120
In your company, two departments with separate GCP projects (code-dev and data-dev) in the same organization need to allow full cross-communication between all of their virtual machines in GCP. Each department has one VPC in its project and wants full control over their network. Neither department intends to recreate its existing computing resources. You want to implement a solution that minimizes cost.
Which two steps should you take? (Choose two.)

A. Connect both projects using Cloud VPN.
B. Connect the VPCs in project code-dev and data-dev using VPC Network Peering.
C. Enable Shared VPC in one project (
D. g., code-dev), and make the second project (
E. g., data-dev) a service project.
F. Enable firewall rules to allow all ingress traffic from all subnets of project code-dev to all instances in project data-dev, and vice versa.
G. Create a route in the code-dev project to the destination prefixes in project data-dev and use nexthop as the default gateway, and vice versa.

Answer: BD

NEW QUESTION 125
Your organization has a Google Cloud Virtual Private Cloud (VPC) with subnets in us-east1, us-west4, and europe-west4 that use the default VPC configuration. Employees in a branch office in Europe need to access the resources in the VPC using HA VPN. You configured the HA VPN associated with the Google Cloud VPC for your organization with a Cloud Router deployed in europe-west4. You need to ensure that the users in the branch office can quickly and easily access all resources in the VPC. What should you do?

A. Create custom advertised routes for each subnet.
B. Configure each subnet's VPN connections to use Cloud VPN to connect to the branch office.
C. Configure the VPC dynamic routing mode to Global.
D. Set the advertised routes to Global for the Cloud Router.

Answer: C

NEW QUESTION 127
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual Professional-Cloud-Network-Engineer Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the Professional-Cloud-Network-Engineer Product From:

https://www.2passeasy.com/dumps/Professional-Cloud-Network-Engineer/

Money Back Guarantee

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