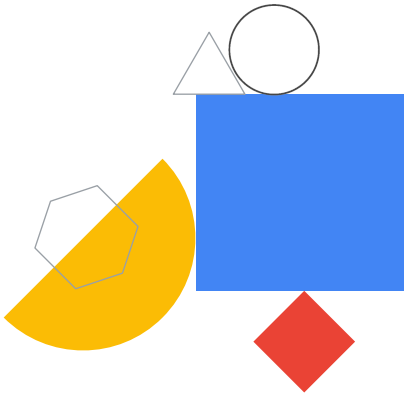
Google Cloud

Preparing for Your Professional Cloud Network Engineer Journey

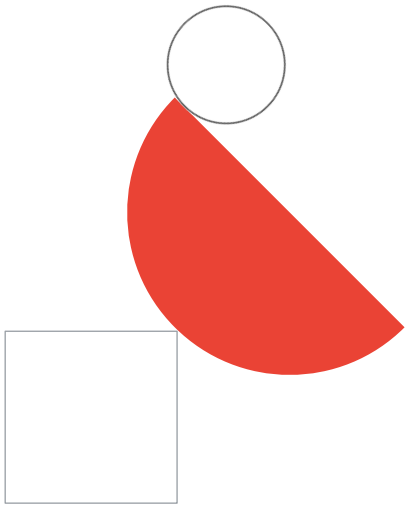


Course Workbook

Certification Exam Guide Sections

1	Designing and planning a Google Cloud network
2	Implementing Virtual Private Cloud (VPC) networks
3	Configuring managed network services
4	Implementing hybrid network interconnectivity
5	Managing, monitoring, and troubleshooting network operations

Section 1:
Designing and planning a Google Cloud network



1.1 Diagnostic Question 01

You are a network engineer designing a network IP plan and need to select an IP address range to use for a subnet. The subnet will need to host up to 2000 virtual machines, each to be assigned one IP address from the subnet range. It will also need to fit in the network IP range 10.1.0.0/16 and be as small as possible.

What subnet range should you use?

A. 10.1.1.0/24
B. 10.1.240.0/21
C. 10.1.1.0/21
D. 10.1.240.0/20

1.1 Diagnostic Question 02

Cymbal Bank has a network support engineering team which will need access to create or change subnet names, locations, and IP address ranges for some but not all subnetworks of a VPC network in a Google Cloud project. Cymbal Bank uses the principle of least privilege and would like to restrict role usage to Google predefined roles.

Which role should be assigned to this group?

A. The Compute Admin role bound at the project level for the project that owns the VPC network

B. The Compute Network Admin role bound at the project level for the Project that owns the VPC network

C. The Compute Network Admin role bound at the resource level for the subnetworks of the VPC network that will be created or changed by the team

D. The Compute Admin role bound at the resource level for the subnetworks of the VPC network that will be created or changed by the team

1.1 Diagnostic Question 03

You are a network engineer designing a solution for hosting a Cymbal Bank web application in Google Cloud. The application will serve a collection of static and dynamic web resources served over HTTPS to users worldwide. You need to design a solution that maximizes availability while minimizing average user latency.

Which of the following features of Google Cloud networking can you utilize? (Select 2)

A. Cloud CDN could be used to cache static content resources at edge locations close to end-users, increasing their availability and minimizing their latency.

B. Cloud NAT could be used to provide outbound connectivity to the internet for resources with only internal IP addresses, thereby increasing their availability.

C. Google Cloud Armor could be used to provide protection against DDoS and injection attacks and thereby minimize solution latency.

D. An Application Load Balancer with a backend service connected to a set of regional MIGs, distributed over the regions closest to the users, to improve availability and minimize latency.

E. Network Intelligence Center could be used to provide network insights, enabling the web application to be deployed in a configuration with maximum availability and minimal latency.

1.1 Designing an overall network architecture

Courses

Networking in Google Cloud
- M5 Private Connection Options
- M9 Controlling Access to VPC Networks
- M11 Hybrid Load Balancing and Traffic Management
- M12 Caching and Optimizing Load Balancing

Networking in Google Cloud: Network Security
- M2 Controlling Access to VPC Networks

Networking in Google Cloud: Routing and Addressing
- M2 Private Connection Options

Networking in Google Cloud: Load Balancing
- M1 Hybrid Load Balancing and Traffic Management
- M2 Caching and Optimizing Load Balancing

Skill Badge

Documentation

Compute Engine IAM roles and permissions

Cloud CDN overview

Cloud NAT overview

Cloud Load Balancing overview

Google Cloud Armor overview

Network Intelligence Center

1.2 Diagnostic Question 04

Cymbal Bank needs to create one or more VPC networks to host their cloud services in 3 regions: Northeastern US, Western Europe, and Southeast Asia. The services require bi-directional inter-regional communication on port 8443. The services receive external internet traffic on port 443.

What is the minimal network topology in Google Cloud that would satisfy these requirements?

A. 3 custom VPC networks, one in each region with one subnet each. The VPC networks all connected with VPC peering with default firewall rules, and custom routes added to support the traffic requirements.

B. 3 custom VPC networks, one in each region with one subnet each. The VPC networks all connected with VPC peering with default routes, and firewall rules added to support the traffic requirements.

C. 1 custom VPC network, with a subnet in each region. The VPC network has the default routes, and the appropriate firewall rules added to support the traffic requirements.

D. 1 custom VPC network, with a subnet in each region. The VPC network has default firewall rules and custom routes added to support the traffic requirements.

1.2 Diagnostic Question 05

Sarah is a network architect responsible for the network design between Cymbal Bank's on-premises network and Google Cloud resources, and also between Cymbal Bank's Google Cloud resources and a partner company's Google Cloud resources. These connections must provide private IP connectivity and support up to 100 Gbps of data exchange with minimum possible latency.

Which options satisfy these requirements? (Select 2)

A. A Shared VPC network connecting Google Cloud resources for Cymbal Bank and the partner company

B. VPC peering between VPC networks for Cymbal Bank and the partner company

C. A Dedicated Interconnect connection between Cymbal Bank's on-premises network and their Google Cloud VPC network

D. A Cloud VPN tunnel between Cymbal Bank's on-premises network and their Google Cloud VPC network

E. 50 Cloud VPN tunnels between Cymbal Bank's on-premises network and their Google Cloud VPC network

1.2 Diagnostic Question 06

You are selecting Google Cloud locations to deploy Google Cloud VMs. You have general requirements to maximize availability and reduce average user latency with a lower priority goal of reducing networking costs. The users served by these VMs will be in Toronto and Montreal. You must deploy workloads requiring instances at 99.5% availability in Toronto and 99.99% availability in Montreal. These instances all exchange a large amount of traffic among themselves.

Which deployment option satisfies these requirements?

A. Deploy instances in multiple zones in the northamerica-northeast1 (Montreal) and northamerica-northeast2 (Toronto) regions.

B. Deploy instances in a single zone in the northamerica-northeast1 (Montreal) and northamerica-northeast2 (Toronto) regions.

C. Deploy instances in a single zone in the northamerica-northeast1 (Montreal) region and multiple zones in the northamerica-northeast2 (Toronto) region.

D. Deploy instances in multiple zones in the northamerica-northeast1 (Montreal) region and a single zone in the northamerica-northeast2 (Toronto).

1.2 Designing Virtual Private Cloud (VPC) networks

Courses

Networking in Google Cloud
- M2 Sharing VPC Networks
- M5 Private Connection Options
- M6 Introduction to Network Architecture
- M7 Network Topologies
- M13 Connectivity Options

Networking in Google Cloud: Fundamentals
- M2 Sharing VPC Networks

Networking in Google Cloud: Routing and Addressing
- M2 Private Connection Options

Networking in Google Cloud: Network Architecture
- M1 Introduction to Network Architecture
- M2 Network Topologies

Networking in Google Cloud: Hybrid and Multicloud
- M1 Connectivity Options

Skill Badge

Google Cloud

Networking Fundamentals in Google Cloud

Documentation

VPC network overview
VPC firewall rules overview
Routes overview | VPC
Shared VPC overview
VPC Network Peering overview
Choosing a Network Connectivity product
Global Locations - Regions & Zones
Regions and zones | Compute Engine Documentation
Global, regional, and zonal resources | Compute Engine Documentation
All networking pricing | Virtual Private Cloud
Compute Engine Service Level Agreement (SLA)

1.3 Diagnostic Question 07

You are designing a VPN solution to connect Cymbal Bank's on-premises data center to Google Cloud. You have a BGP-capable VPN gateway installed in the data center and require 99.99% availability for the VPN link.

What Cloud VPN configuration meets these requirements while requiring the least setup and maintenance?

A. Classic VPN with route-based static routing
B. Classic VPN with policy-based static routing
C. Classic VPN with Cloud Router and dynamic routing
D. HA VPN with Cloud Router and dynamic routing

1.3 Diagnostic Question 08

To reduce latency, you will be replacing an existing Cloud VPN Classic VPN connection. You will connect your organization's on-premises data center to Google Cloud resources in a VPC network with all resources in a single subnet and region using private/internal IP connectivity. The connection will need to support 1.5 Gbps of traffic. Due to cost considerations, you would like to order the option that provides just enough bandwidth and not more but must have significantly lower latency than the existing Cloud VPN connection.

What should you use?

A. A 10 Gbps Dedicated Interconnect connection with one 10 Gbps VLAN attachments

B. A 2 Gbps Dedicated Interconnect connection with one 2 Gbps VLAN attachments

C. A Partner Interconnect connection with 1 or 2 VLAN attachments

D. A Cloud VPN HA VPN connection with Cloud Router

1.3 Designing a resilient and performant hybrid and multi-cloud network

Courses

Networking in Google Cloud

- M13 Connectivity Options
- M14 Cloud VPN

Networking in Google Cloud: Hybrid and Multicloud

- M1 Connectivity Options
- M2 Cloud VPN

Documentation

Cloud VPN overview
Cloud Interconnect overview
Dedicated Interconnect overview
Partner Interconnect overview
Key terms | Cloud Interconnect
Pricing | Cloud Interconnect
Choosing a Network Connectivity product

1.4 Diagnostic Question 09

You need to create a GKE cluster, be able to connect to pod IP addresses from your on-premises environment, and control access to pods directly using firewall rules. You will need to support 300 nodes, 30000 pods, and 2000 services.

Which configuration satisfies these requirements?

A. A GKE route-based cluster in a subnet with primary IP range 10.0.240.0/20 and pod IP range of 10.1.0.0/16

B. A GKE route-based cluster in a subnet with primary IP range 10.0.240.0/20 and pod IP range of 10.252.0.0/14

C. A GKE VPC-native cluster in a subnet with primary IP range 10.0.240.0/20, pod IP range of 10.252.0.0/15, and service IP range of 10.0.224.0/20

D. A GKE VPC-native cluster in a subnet with primary IP range 10.0.240.0/20, pod IP range of 10.252.0.0/16, and service IP range of 10.0.224.0/20

1.4 Diagnostic Question 10

Cymbal Bank wants to ensure communication from their on-premises data centers to the GKE control plane stays private using internal IP communication and their Dedicated Interconnect links. However, they will need to allow administrators to periodically connect to the cluster control plane from remote internet-accessible locations that don't have access to the on-premises private network. You want to select a configuration and connection approach that will enable these requirements while providing the highest security.

What should you do?

A. Deploy a private GKE cluster with public endpoint access enabled and authorized networks disabled.

B. Deploy a private GKE cluster with public endpoint access enabled and authorized networks enabled. Configure authorized networks for the cluster to include all remote source IP ranges that administrators may connect from.

C. Deploy a private GKE cluster with public endpoint access disabled. Create a VM in the same subnet with only an internal IP address and provide IAP tunnel based SSH access to remote administrators for this VM. Have remote administrators connect via IAP tunnel SSH to this VM when requiring access to the GKE cluster control plane.

D. Deploy a private GKE cluster with public endpoint access disabled. Provide remote administrators IAP tunnel based SSH access to a node in the cluster. Have remote administrators connect via an IAP tunnel SSH to this node when requiring access to the GKE cluster control plane.

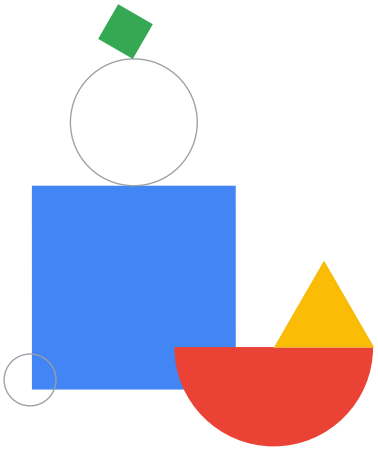
1.4 Designing an IP addressing plan for Google Kubernetes Engine

Skill Badge

Documentation

- Types of clusters | Kubernetes Engine Documentation
- VPC-native clusters | Kubernetes Engine Documentation
- Creating a VPC-native cluster | Kubernetes Engine Documentation
- Creating a routes-based cluster | Kubernetes Engine Documentation
- Private clusters | Kubernetes Engine Documentation
- Creating a private cluster | Kubernetes Engine Documentation

Google Cloud



Section 2: Implementing Virtual Private Cloud (VPC) networks

2.1 Diagnostic Question 01

Cymbal Bank has a custom VPC network with two subnets (in us-central1 and us-east1) each hosting 500 VMs. The primary ranges for each are 10.128.128.0/23 and 10.128.192.0/23. The VPC has default routes and three firewall rules (all at priority 1000): (A) allows ingress on TCP port 443 from any IP address; (B) allows ingress on TCP port 8443 from the primary ranges of each subnet; and (C) denies egress to the primary ranges for each subnet for all ports and protocols except for TCP port 8443. To reduce networking costs, Cymbal Bank wants to consolidate the 1000 VMs into a single subnet in us-central1 (and use a primary IP range for that subnet to support that) and delete the us-east1 subnet. You want to ensure the simplest possible firewall rules in the new configuration that provide the same traffic control.

Select the sequence of configuration steps that can accomplish this with minimal interruption to the workloads.

A. Create a new subnet in us-central1 with primary IP range 10.128.128.0/22; delete the VMs in the existing subnets one at a time and re-create them in the new subnet; delete the old subnets; and update the B and C firewall rules to use the single new subnet primary range.

B. Create a new subnet in us-central1 with primary IP range 10.192.128.0/22; delete the VMs in the existing subnets one at a time and re-create them in the new subnet; delete the old subnets; and update the B and C firewall rules to use the single new subnet primary range.

C. Expand the subnet in us-central1 to a primary IP range 10.128.128.0/22; delete the VMs in the us-east1 subnet one at a time and re-create them in the us-central1 subnet; delete the us-east1 subnet; and update the B and C firewall rules to use the single us-central1 subnet primary range.

D. Expand the existing subnet in us-central1 to a primary IP range 10.192.128.0/22; delete the VMs in the us-east1 subnet one at a time and re-create them in the us-central1 subnet; delete the us-east1 subnet; and update the B and C rules to use the single us-central1 subnet primary range.

2.1 Diagnostic Question 02

You are designing a networking scheme for Cymbal Bank with the requirement to use internal IP addresses for communication, with the lowest possible latency. Cymbal Bank has several teams, each with its own projects: P1, P2, and P3. Cymbal Bank would like consolidated network billing, administration, and access control for the cloud environment. VMs in these projects need to connect to VMs in a partner organization in projects P4 and P5.

Select the networking option that best satisfies these requirements.

A. Connect the VMs across the projects and partner organization VPCs in each project (V1, V2, V3, V4, V5) using and VPC peering (peering V1 to V2, V2 to V3, V3 to V4, and V4 to V5).

B. Connect the VMs across the Cymbal projects (P1-P3) using a Shared VPC network (Shared VPC host project P6 with VPC V6, and P1-P3 are the service projects) and then peer that Shared VPC network to the partner organization VPCs (V6 peered to V4 and V4 to V5).

C. Connect the VMs across Cymbal and partner organization projects (P1-P5) using a Shared VPC network (Shared VPC host project P6 with VPC V6, and P1-P5 are the service projects).

D. Connect the VMs across the Cymbal projects (P1-P3) using a Shared VPC network (Shared VPC host project P6 with VPC V6, and P1-P3 are the service projects) and then peer that Shared VPC network to the partner organization VPCs (V6 peered to V4 and V6 to V5).

2.1 Configuring VPCs

Courses

Networking in Google Cloud
- M1 VPC Networking Fundamentals
- M2 Sharing VPC Networks
- M5 Private Connection Options
- M9 Controlling Access to VPC Networks

Networking in Google Cloud: Fundamentals
- M1 VPC Networking Fundamentals
- M2 Sharing VPC Networks

Networking in Google Cloud: Routing and Addressing
- M2 Private Connection Options

Networking in Google Cloud: Network Security
- M2 Controlling Access to VPC Networks

Skill Badges

Google Cloud
Implement Cloud Security Fundamentals on Google Cloud

Google Cloud
Networking Fundamentals in Google Cloud

Google Cloud
Build a Secure Google Cloud Network

Documentation

VPC network overview

Using VPC networks

VPC firewall rules overview

Using firewall rules | VPC

2.2 Diagnostic Question 03

Cymbal Bank needs to connect two on-premises networks to a single VPC network in Google Cloud. One on-premises network supports BGP routing and is located near the us-central1 region. The other on-premises network does not support BGP routing and is located near us-east1. The VPC network has subnets in each of these regions. You will use Cloud VPN to enable private communication between the on-premises networks and the VPC network.

Select the configuration that provides the highest availability and the lowest average latency.

A. Configure the VPC for regional dynamic routing mode; create a Cloud Router in each of the two regions; and connect each office to its closest region via an HA VPN gateway with dynamic routing in that region.

B. Configure the VPC for regional dynamic routing mode; create one Cloud Router in the us-central1 region; connect the office close to us-central1 to the VPC using an HA VPN gateway with dynamic routing in us-central1; and connect the other office via a Classic VPN gateway using static routing in us-east1.

C. Configure the VPC for global dynamic routing mode; create Cloud Routers in each of the two regions; and connect each office to its closest region via an HA VPN gateway with dynamic routing in that region.

D. Configure the VPC for global dynamic routing mode; create Cloud Routers in each of the two regions; connect the office close to us-central1 to the VPC using an HA VPN gateway with dynamic routing in us-central1; and connect the other office via a Classic VPN gateway using static routing in us-east1.

2.2 Diagnostic Question 04

You are designing a VPC network with the requirement that all external traffic destined for the internet is passed through a proxy VM. The proxy will have software installed to scan, detect, and drop invalid egress traffic and to help prevent data exfiltration, outbound attacks, or access to blocked websites.

Select the configuration that can most easily accomplish this.

A. Create a custom route to the destination 0.0.0.0/0, and specify the next hop as the proxy VM.

B. Delete the system-generated default route, create a custom route to destination 0.0.0.0/0, and specify the next hop as the proxy VM.

C. Create a custom route to the destination 0.0.0.0/0, specify the next hop as the proxy VM, and configure the scanning VM to enable IP forwarding.

D. Delete the system-generated default route, and then create a custom route to destination 0.0.0.0/0. Specify the next hop as the proxy VM, and configure the proxy VM to enable IP forwarding.

2.2 Configuring VPC routing

Courses

Networking in Google Cloud
- M4 Network Routing and Addressing
- M13 Connectivity Options
- M14 Cloud VPN

Networking in Google Cloud: Routing and Addressing
- M1 Network Routing and Addressing

Networking in Google Cloud: Hybrid and Multicloud
- M1 Connectivity Options
- M2 Cloud VPN

Skill Badges

Google Cloud
Build a Secure Google Cloud Network

Google Cloud
Implement Cloud Security Fundamentals on Google Cloud

Google Cloud
Network Performance and Optimization

Documentation

Cloud VPN overview
Best practices for Cloud VPN
HA VPN topologies
Classic VPN topologies
Creating an HA VPN gateway to a peer VPN gateway
Creating an HA VPN between Google Cloud networks
Creating a Classic VPN using static routing
Networks and tunnel routing | Cloud VPN
Cloud Router overview
Routes overview | VPC
Using routes | VPC

2.3 Diagnostic Question 05

Cymbal Bank is experiencing network performance issues, security concerns, and difficulties in scaling their network to support new branches. Their current network infrastructure includes a mix of on-premises and cloud-based resources, with multiple vendors and complex interconnections.

Given Cymbal Bank's complex network environment and specific challenges, which of the following strategic approaches would most effectively address their requirements for network performance, security, and scalability while minimizing operational overhead and disruption to business operations?

Select the configuration that can address all of the above requirements.

A. Implement a hybrid cloud networking solution with advanced routing protocols to optimize traffic flow and reduce latency.

B. Adopt a zero-trust security architecture and leverage microsegmentation to enhance network security and protect sensitive data.

C. Deploy Network Connectivity Center with Cloud VPN to create a centralized network management platform and establish secure, high-performance connections between branches and the cloud.

D. Utilize Cloud Interconnect to establish dedicated network connections between on-premises data centers and Google Cloud for improved performance and reliability.

2.3 Configuring Network Connectivity Center

Courses

Networking in Google Cloud
- M14 Cloud VPN

Networking in Google Cloud: Hybrid and Multicloud
- M2 Cloud VPN

Documentation

Network Connectivity Center overview

Private NAT for Network Connectivity Center spokes | Google Cloud

Set up and manage network address translation with Private NAT | Google Cloud

2.4 Diagnostic Question 06

Cymbal Bank has an existing subnet that you want to use for a new VPC-native GKE cluster. The subnet primary IP address range is 10.128.128.0/20. Currently the 1000 other VMs using that subnet have taken 1000 of the available IP addresses. The new GKE cluster should support 200,000 pods and 30,000 services.

Select the minimal set of configuration steps and the smallest possible IP ranges to enable this.

A. Expand the subnet primary IP address range to 10.128.0.0/16; create a secondary range in the subnet of size /14 for pods and another of size /17 for services; and create the GKE VPC-native cluster in the subnet using these secondary ranges.

B. Create a secondary range in the subnet of size /13 for pods and another of size /16 for services, and create the GKE VPC-native cluster in the subnet using these secondary ranges.

C. Create a GKE VPC-native cluster in the subnet, specifying the size of the pod range as /14 and the size of the services range as /17.

D. Create a GKE VPC-native cluster in the subnet, specifying the size of the pod range as /13 and the size of the services range as /17.

2.4 Diagnostic Question 07

You will be deploying a VPC-native GKE cluster into an existing service project of a Shared VPC. You will create an Ingress to trigger the automatic creation, connection, and firewall configuration of an Application Load Balancer to a service deployed in the cluster for container-native load balancing.

Select the option corresponding to the IAM policy binding of least privilege necessary.

A. Assign the Compute Network User role (in the host project) to the service-{serviceProjectNumber}@container-engine-robot.iam.gserviceaccount.com service account (where serviceProjectNumber is the project number of the service project).

B. Assign the Host Service Agent User (in the host project) to the service-{serviceProjectNumber}@container-engine-robot.iam.gserviceaccount.com service account (where serviceProjectNumber is the project number of the service project) .

C. Assign the Host Service Agent User and the Compute Network User (in the host project) to the service-{serviceProjectNumber}@container-engine-robot.iam.gserviceaccount.com service account (where serviceProjectNumber is the project number of the service project).

D. Assign the Host Service Agent User (in the host project) and the Compute Network User (for the subnet of the GKE cluster in the shared VPC in the host project) to the service-{serviceProjectNumber}@container-engine-robot.iam.gserviceaccount.com service account (where serviceProjectNumber is the project number of the service project).

2.4 Configuring and maintaining Google Kubernetes Engine clusters

Course

Configure Google Kubernetes Engine Networking

- M1 GKE Networking Overview

Skill Badge

Google Cloud

Implement Cloud Security Fundamentals on Google Cloud

Documentation

- Types of clusters | Kubernetes Engine Documentation
- VPC-native clusters | Kubernetes Engine Documentation
- Creating a VPC-native cluster | Kubernetes Engine Documentation
- Optimizing IP address allocation | Kubernetes Engine Documentation
- Setting up clusters with Shared VPC | Kubernetes Engine Documentation
- Network overview | Kubernetes Engine Documentation
- GKE Ingress for HTTP(S) Load Balancing
- Configuring Ingress features | Kubernetes Engine Documentation
- Best practices for GKE networking | Kubernetes Engine Documentation
- Container-native load balancing | Kubernetes Engine Documentation

2.5 Diagnostic Question 08

You are configuring firewall rules for securing a set of microservices (MS1, MS2, MS3) running in separate managed instance groups (MIGs) of VMs in a single subnet of a VPC network. The primary range of the VPC network is 10.128.128.0/20. MS1 will send requests to MS2 on TCP port 8443; MS2 will send requests to MS3 on TCP port 8663; and MS3 will send requests to MS1 on TCP port 8883. There will be no other communication to or between these microservices.

Select a simple and secure firewall configuration to support this traffic requirement.

A. Create service accounts (S1, S2, S3) for the microservices, and assign those service accounts to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source S1 to target S2; for TCP 8663 from source S2 to target S3, and for TCP 8883 from source S3 to target S1.

B. Create network tags (T1, T2. T3) for the microservices, and assign those network tags to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source T1 to target T2; for TCP 8663 from source T2 to target T3; and for TCP 8883 from source T3 to target T4.

C. Create service accounts (S1, S2, S3) for the microservices, and assign those service accounts to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source 10.128.128.0/20 to target S2; for TCP 8663 from source 10.128.128.0/20 to target S3; for TCP and 8883 from source 10.128.128.0/20 to target S1'.

D. Create network tags (T1, T2, T3) for the microservices, and assign those network tags to the instance template for the MIG used by each microservice. Create three ingress allow firewall rules: for TCP 8443 from source 10.128.128.0/20 to target T2; for TCP 8663 from source 10.128.128.0/20 to target T3; and for TCP 8883 from source 10.128.128.0/20 to target T1.

2.5 Diagnostic Question 09

You are trying to determine which firewall rules are incorrectly blocking requests between two VMs running within a VPC network: VM1 and VM2. Firewall logging is enabled for all firewall rules, including metadata. The Firewall Insights and Recommendations API are also enabled. All insights are enabled, and an observation period is set over a period capturing the blocked requests.

Select a valid troubleshooting approach to find the incorrectly configured firewall rule.

A. On the Firewall Insights page of the Google Cloud console, find the names of the deny firewall rules with hits to identify rules that are blocking requests. On the Legacy Logs Viewer or Logs Explorer page, view the firewall logs and filter for logs that match those rules by name, using jsonPayload.rule_details.reference field, matching the names of the deny firewall rules with hits.

B. On the Logs Explorer page, view the firewall logs, and filter for logs that match the source and destination VMs VM1 and VM2, using the jsonPayload.instance.project_id, jsonPayload.instance.vm_name, jsonPayload.instance.region, and jsonPayload.instance.zone, jsonPayload.remote_instance.vm_name, jsonPayload.remote_instance.region, and jsonPayload.remote_instance.zone.

C. On the Logs Explorer or Legacy Logs Viewer page, view the firewall logs, and filter for logs that match the destination VM2 in the VPC, using the jsonPayload.instance.project_id, jsonPayload.instance.vm_name, jsonPayload.instance.region, and jsonPayload.instance.zone fields.

D. On the Firewall Insights landing page of the Google Cloud console, find the names of the allow firewall rules with no hits to identify rules that are not allowing requests. On the Logs Viewer or Explorer page, view the firewall logs and filter for logs matching those rules by name, using jsonPayload.rule_details.reference field (matching the names of the allow firewall rules with no hits).

2.5 Configuring and managing Cloud Next Generation Firewall (NGFW) rules

Courses

Networking in Google Cloud

- M3 Network Monitoring and Logging
- M9 Controlling Access to VPC Networks
- M11 Hybrid Load Balancing and Traffic Management

Networking in Google Cloud: Fundamentals

- M3 Network Monitoring and Logging

Networking in Google Cloud: Network Security

- M2 Controlling Access to VPC Networks

Networking in Google Cloud: Load Balancing

- M1 Hybrid Load Balancing and Traffic Management

Skill Badges

Google Cloud
Build a Secure Google Cloud Network

Google Cloud
Network Performance and Optimization

Google Cloud
Implement Cloud Security Fundamentals on Google Cloud

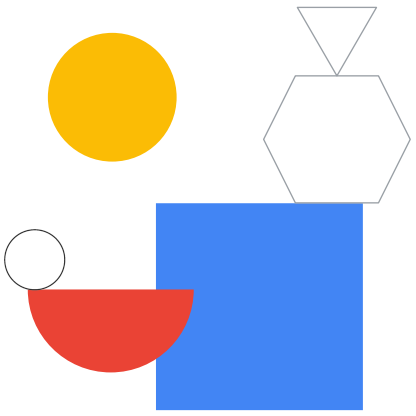
Google Cloud
Networking Fundamentals in Google Cloud

Documentation

- VPC firewall rules overview
- Using firewall rules | VPC
- Firewall Rules Logging overview | VPC
- Using Firewall Rules Logging | VPC
- Using Firewall Insights
- Firewall Insights overview

Google Cloud

Section 3: Configuring managed network services



3.1 Diagnostic Question 01

Cymbal Bank wants a web application to have global anycast load balancing across multiple regions. The web application will serve static asset files and will also use REST APIs that serve dynamic responses. The load balancer should support HTTP and HTTPS requests and redirect HTTP to HTTPS. The load balancer should also serve all the requests from the same domain name, with different paths indicating static versus dynamic resources.

Select the load balancer configuration that would most effectively enable this scenario.

A. A global external Application Load Balancer with one global forwarding rule, forwarding to one target proxy with one URL map connected to two backend services

B. A global external Application Load Balancer with two global forwarding rules, forwarding to two target proxies: one with URL map and no backend service, and the other with URL map and two backend services

C. Two global external Application Load Balancers, each with one global forwarding rule forwarding to one target proxy with one URL map connected to one backend service

D. A global external Application Load Balancer with two global forwarding rules forwarding to two target proxies: one with URL map and no backend service, and the other with URL map, one backend service, and one backend bucket

3.1 Diagnostic Question 02

You are designing a load balanced autoscaling frontend for Cymbal Bank. It is intended to be deployed into Google Kubernetes Engine (GKE). You want to use container-native load balancing and autoscale based on the amount of traffic to the service.

Select the type of backend and autoscaling that would accomplish this.

A. A managed instance group of GKE nodes that autoscale using cluster autoscaling
B. A zonal network endpoint group of Kubernetes pods that autoscale using a Horizontal Pod Autoscaler
C. A managed instance group of GKE nodes that contain pods that autoscale using a Horizontal Pod Autoscaler
D. A serverless network endpoint group of GKE pods that autsocale using a Horizontal Pod Autoscaler

3.1 Configuring load balancing

Courses

Networking in Google Cloud
- M11 Hybrid Load Balancing and Traffic Management

Networking in Google Cloud: Load Balancing
- M1 Hybrid Load Balancing and Traffic Management

Skill Badges

Google Cloud
Build a Secure Google Cloud Network

Google Cloud
Implement Load Balancing on Compute Engine

Google Cloud
Networking Fundamentals in Google Cloud

Documentation

Cloud Load Balancing overview
Choosing a load balancer
Load balancer feature comparison
External Application Load Balancer overview
Internal Application Load Balancer overview
Backend service-based external passthrough Network Load Balancer overview
Internal passthrough Network Load Balancer overview
External proxy Network Load Balancer overview
Backend services overview
Forwarding rules overview
Instance groups
Creating managed instance groups
Network endpoint groups overview
Zonal network endpoint groups overview
Internet network endpoint groups overview
Serverless network endpoint groups overview

3.2 Diagnostic Question 03

Cymbal Bank wants to protect their services, which are deployed behind an Application Load Balancer, from L7 distributed denial of service (DDoS), SQL injection (SQLi), and cross-site scripting (XSS) attacks.

A. Configure Google Cloud Armor with the appropriate rules.
B. Configure a VM with appropriate scanning and filtering software in front of the Application Load Balancer.
C. Configure Google Cloud WAF with the appropriate rules.
D. Configure Cloud NAT with the appropriate rules.

Select the simplest approach to accomplish this.

3.2 Configuring Google Cloud Armor policies

Courses

Networking in Google Cloud
- M11 Hybrid Load Balancing and Traffic Management
- M12 Caching and Optimizing Load Balancing

Networking in Google Cloud: Load Balancing
- M1 Hybrid Load Balancing and Traffic Management
- M2 Caching and Optimizing Load Balancing

Skill Badges

Google Cloud
Build a Secure Google Cloud Network

Google Cloud
Networking Fundamentals in Google Cloud

Documentation

Security policy overview

Configuring Google Cloud Armor security policies

Google Cloud Armor custom rules language reference

Tuning Google Cloud Armor WAF rules

3.3 Diagnostic Question 04

Cymbal Bank uses Cloud CDN to cache a web application served from a backend bucket connected to a Cloud Storage bucket. You need to cache all the web-app files with appropriate time to live (TTL) except for the index.html file. The index.html file contains links to versioned files and should always be fetched or re-validated from the origin.

Select the configuration option to satisfy these requirements with minimal effort.

A. Set the Cloud CDN cache mode for the backend bucket to CACHE_ALL_STATIC.

B. Set the Cloud CDN cache mode for the backend bucket to FORCE_CACHE_ALL, and ensure that the Cache-Control metadata for index.html is set to private.

C. Set the Cloud CDN cache mode for the backend bucket to CACHE_ALL_STATIC, and ensure that the Cache-Control metadata for index.html is not set or is set to no-store, no-cache, or private.

D. Set the Cloud CDN cache mode to USE_ORIGIN_HEADERS, set the Cache-Control metadata for index.html to no-store, and set the Cache-Control headers for all the other files with appropriate TTL values.

3.3 Diagnostic Question 05

Cymbal Bank is serving files from a backend bucket and wants to ensure time-limited read access without authentication. The backend bucket uses signed URLs to access those files. The files are also being cached in Cloud CDN. There is a problem with one of the files, and you want to delete it. You also want to immediately ensure no read access via the signed URL to the cached file copy in Cloud CDN, although the expiry time is currently set to sometime in the future.

Select the option that accomplishes this with lowest cost and effort.

A. Perform cache invalidation for the file using the full path.

B. Perform cache invalidation for the file using the path and excluding the query parameters used for the signed URL.

C. Update the expiry time for the signed URL to be the current time.

D. Delete the key used to create the signed URL.

3.3 Configuring Cloud CDN

Courses

Networking in Google Cloud
- M12 Caching and Optimizing Load Balancing

Networking in Google Cloud: Load Balancing
- M2 Caching and Optimizing Load Balancing

Skill Badge

Google Cloud

Network Performance and Optimization

Documentation

Cloud CDN overview

Cloud CDN features

Best practices for content delivery | Cloud CDN

Caching overview | Cloud CDN

Signed URLs and signed cookies overview | Cloud CDN

Using signed URLs | Cloud CDN

Using signed cookies | Cloud CDN

Cache invalidation overview | Cloud CDN

Invalidating cached content | Cloud CDN

3.4 Diagnostic Question 06

Cymbal Bank will use a hybrid DNS approach. Cymbal has a VPC in Google Cloud that connects to their on-premises networks via Interconnect. You will use Cloud DNS for Cymbal's public DNS zone at cymbalbank.com and also for private DNS for resources at gcp.cymbalbank.com. You will use Cymbal's on-premises DNS, which is configured as authoritative for on-premises private resources at corp.cymbalbank.com.

Select the Cloud DNS managed zone configuration that will satisfy the requirements.

A. Create a single Cloud DNS managed zone in Google Cloud that is configured for private DNS for gcp.cymbalbank.com and public DNS for cymbalbank.com and that also acts as a forwarding zone to the on-premises DNS for corp.cymbalbank.com DNS requests.

B. Create a Cloud DNS private managed zone for gcp.cymbalbank.com, a public managed zone for cymbalbank.com, and a third forwarding zone for corp.cymbalbank.com that forwards DNS requests to the on-premises DNS.

C. Create a public managed zone for cymbalbank.com and a Cloud DNS private managed zone for gcp.cymbalbank.com that also forwards DNS requests for corp.cymbalbank.com to the on-premises DNS.

D. Create a Cloud DNS private managed zone for gcp.cymbalbank.com and a public managed zone for cymbalbank.com that also forwards DNS requests for corp.cymbalbank.com to the on-premises DNS.

3.4 Diagnostic Question 07

You are configuring hybrid DNS for Google Cloud using Cloud DNS and your on-premises DNS. You have three VPC networks in Google Cloud in three different projects that should forward DNS requests for a particular private domain to the on-premises DNS. All three projects have Cloud VPN connections to the on-premises network.

Select the Google recommended approach for enabling this requirement.

A. For the VPC in one of the projects, create a Cloud DNS forwarding zone for its VPC. For the VPC in each of the other projects, create a Cloud DNS peering zone that targets the VPC with the forwarding zone.

B. Create a forwarding zone in one of the projects that is visible to the VPCs in all of the projects.

C. Create a forwarding zone in each of the projects that is visible to the VPC in that project.

D. Create a forwarding zone and a peering zone in each project. Make the forwarding zone visible to the VPC in the same project and the peering managed zones associated with the VPCs in the other projects.

3.4 Configuring and maintaining Cloud DNS

Courses

Networking in Google Cloud

- M4 Network Routing and Addressing

Networking in Google Cloud: Routing and Addressing

- M1 Network Routing and Addressing

Documentation

Cloud DNS overview
General DNS overview
DNS best practices
Key terms | Cloud DNS
Manage zones | Cloud DNS
Manage records | Cloud DNS
DNS Security Extensions (DNSSEC) overview
Name resolution order | Cloud DNS
DNS policies overview
Cross-project binding zones | Cloud DNS
DNS server policies
Manage response policies and rules | Cloud DNS
Manage DNS routing policies

3.5 Diagnostic Question 08

Cymbal is using Cloud NAT to provide internet connectivity to a group of VMs in a subnet. There are 500 VMs in the subnet, and each VM may have up to 1000 internet bound connections simultaneously.

What Cloud NAT configuration will support this requirement?

A. Set the minimum ports per VM to 1000, and set the number of IP addresses used by the Cloud NAT Gateway to 8.

B. Set the minimum ports per VM to 2000, and set the number of IP addresses used by the Cloud NAT Gateway to 8.

C. Set the minimum ports per VM to 2000, and set the number of IP addresses used by the Cloud NAT Gateway to 10.

D. Set the minimum ports per VM to 1000, and set the number of IP addresses used by the Cloud NAT Gateway to 6.

3.5 Configuring and securing Internet egress traffic

Courses

Networking in Google Cloud

- M5 Private Connection Options

Networking in Google Cloud: Routing and Addressing

- M2 Private Connection Options

Documentation

Cloud NAT overview
Cloud NAT address and port overview
Configure Cloud NAT
Example Compute Engine setup | Cloud NAT
Using Cloud NAT rules

3.6 Diagnostic Question 09

You are designing a system in Google Cloud to ensure that all traffic being sent between two subnets is passed through a security gateway VM. The VM runs third-party software that scans traffic for known attack signatures and then forwards or drops traffic based on the scan results.

Select a configuration that satisfies these requirements.

A. Create the two subnets in the same VPC. Create a VM running the third-party scanning software in one of the subnets. Create custom routes in the VPC to send traffic for each subnet from the opposite subnet through that VM.

B. Create the two subnets in the same VPC. Create a VM running the third-party scanning software in each of the subnets. Create custom routes in the VPC to send traffic destined for each subnet originating in the opposite subnet through the VM in its subnet.

C. Create the two subnets in two separate VPCs. Create a VM with two network interfaces (NICs), with each NIC connected to the subnet in each VPC. Create custom routes in each VPC to send traffic destined for each subnet originating in the opposite subnet through the VM.

D. Create the two subnets in the same VPC. Create two VMs running the third-party scanning software, with one in each of the subnets. Create custom routes in the VPC to send traffic destined for each subnet originating in the opposite subnet through the VM in the opposite subnet.

3.6 Diagnostic Question 10

Select the list of the resources that must be created or configured to enable packet mirroring.

A. A packet mirroring policy and a collector instance

B. A packet mirroring policy, an internal passthrough Network Load Balancer configured for packet mirroring, an instance group of collector instances, and firewall rules

C. A packet mirroring policy, a collector instance, and firewall rules

D. A packet mirroring policy, an instance group of collector instances, and firewall rules

3.6 Configuring network packet inspection

Courses

Networking in Google Cloud
- M1 VPC Networking Fundamentals
- M3 Network Monitoring and Logging
- M10 Advanced Security Monitoring and Analysis

Networking in Google Cloud: Fundamentals
- M1 VPC Networking Fundamentals
- M3 Network Monitoring and Logging

Networking in Google Cloud: Network Security
- M3 Advanced Security Monitoring and Analysis

Skill Badges

Google Cloud
Implement Cloud Security Fundamentals on Google Cloud

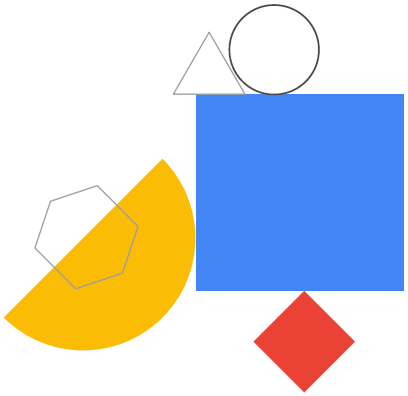
Google Cloud
Networking Fundamentals in Google Cloud

Documentation

- Multiple network interfaces overview and examples | VPC
- Creating instances with multiple network interfaces | VPC
- Internal TCP/UDP load balancers as next hops | Load Balancing
- Setting up Internal TCP/UDP Load Balancing for third-party appliances
- Packet Mirroring overview | VPC
- Using Packet Mirroring | VPC
- Monitoring Packet Mirroring | VPC
- Internal passthrough Network Load Balancer overview

Google Cloud

Section 4: Implementing hybrid network interconnectivity



4.1 Diagnostic Question 01

Cymbal Bank is configuring a Layer 3 Partner Interconnect connection to Google Cloud.

Select the sequence of high-level activities you will need to perform in order to accomplish this.

A. Establish connection to selected partner service provider. Create and activate VLAN attachments and Google-generated pairing keys. Request VLAN attachments providing pairing keys. ...receive connections for

B. Establish connection to selected partner service provider. Create and activate VLAN attachments and receive Google-generated pairing keys. Request connections for VLAN attachments from partner specifying region and capacity and providing attachment pairing key. Configure BGP for on-premises routers.

C. Establish connection to selected partner service provider. Create VLAN attachments and receive Google-generated pairing keys. Request connections for VLAN attachments from partner specifying region and capacity and providing attachment pairing key. Activate VLAN attachments. Configure BGP for on-premises routers.

D. Establish connection to selected partner service provider. Create VLAN attachments and receive Google-generated pairing keys. Request connections for VLAN attachments from partner specifying region and capacity and providing attachment pairing key. Activate VLAN attachments.

4.1 Diagnostic Question 02

You are setting up a Dedicated Interconnect connection and need to provide the highest capacity possible.

Select the circuit configuration that achieves this.

A. 1 200 Gbps circuit
B. 2 100 Gbps circuits
C. 8 10 Gbps circuits
D. 8 50 Gbps circuits

4.1 Diagnostic Question 03

Cymbal Bank wants to achieve 99.9% availability with Dedicated Interconnect. You want to support 100 Gbps of throughput, even if a single interconnect connection were to fail.

Select the simplest and least expensive configuration that can meet these requirements.

A. 2 100 Gbps connections in separate edge availability zones of the co-location facility, 4 50 Gbps VLAN attachments

B. 2 100 Gbps connections in separate edge availability zones of the co-location facility, 2 100 Gbps VLAN attachments

C. 1 200 Gbps connection in a single edge availability zone of the co-location facility, 4 50 Gbps VLAN attachments

D. 2 50 Gbps connections in separate edge availability zones of the co-location facility, 4 25 Gbps VLAN attachments

4.1 Configuring Google Cloud Interconnect

Courses

Networking in Google Cloud

- M13 Connectivity Options

Networking in Google Cloud: Hybrid and Multicloud

- M1 Connectivity Options

Documentation

Best practices for Cloud Interconnect

Key terms | Cloud Interconnect

Partner Interconnect overview

Partner Interconnect provisioning overview

Creating VLAN attachments | Cloud Interconnect

Requesting connections | Cloud Interconnect

Activating connections | Cloud Interconnect

Configuring on-premises routers | Cloud Interconnect Best practices for Cloud Interconnect

Creating VLAN attachments | Partner Interconnect

Creating VLAN attachments | Dedicated Interconnect

Establishing 99.99% availability for Dedicated Interconnect

Establishing 99.99% availability for Partner Interconnect

Establishing 99.9% availability for Dedicated Interconnect

Establishing 99.9% availability for Partner Interconnect

4.2 Diagnostic Question 04

Cymbal Bank is connecting one of their Shared VPC networks to their on-premises network via Dedicated Interconnect.

Select the recommended approach for configuring their VLAN attachments and Cloud Routers.

A. Create the Cloud Routers in the Shared VPC host project and the VLAN attachments in the Shared VPC service projects.
B. Create the VLAN attachments and Cloud Routers in the Shared VPC host project.
C. Create the VLAN attachments in the Shared VPC host project and the Cloud Routers in the Shared VPC service projects.
D. Create the VLAN attachments and Cloud Routers in the Shared VPC service projects.

4.2 Diagnostic Question 05

Cymbal Bank is connecting a branch office with an old VPN gateway that doesn't support BGP. The old VPN gateway only supports IKEv1 and does not support local and remote traffic selectors to be configured as 0.0.0.0/0.

Select the configuration option that can satisfy these requirements.

A. Configure an HA VPN gateway to connect to the on-premises gateway and use dynamic routing.

B. Configure a Classic VPN gateway to connect to the on-premises gateway using static routing with a route-based tunnel.

C. Configure a Classic VPN gateway to connect to the on-premises gateway using static routing with a policy-based tunnel with local and remote traffic selectors matching the office VPN but reversed.

D. Configure a Classic VPN gateway to connect to the on premise gateway and use dynamic routing.

4.2 Diagnostic Question 06

You are using the gcloud tool to create a Classic VPN with static routing and a route-based tunnel. The on-premises resources are all in the 192.168.1.0/24 range. You have issued commands to create the VPN gateway, IP addresses, forwarding rules, and the VPN tunnel.

Select the correct final resource that must be created.

A. A Cloud Router with default route advertisements
B. A Cloud Router with a custom route advertisements including the range 192.168.1.0/24
C. A route with destination 192.168.1.0/24 and next hop set to the VPN gateway
D. A route with destination 0.0.0.0/0 and next hop set to the VPN gateway

4.2 Diagnostic Question 07

Cymbal Bank is connecting a branch office with a modern VPN gateway that supports BGP to Google Cloud in a region. The office VPN gateway has two interfaces and only requires a single tunnel to each to provide 99.99% availability.

Select the simplest Google Cloud VPN configuration that will provide 99.99% availability.

A. An external VPN gateway resource with 2 interfaces, a Cloud Router in the same region, a cloud HA VPN gateway with one tunnel from each interface to each external VPN gateway interface, and BGP sessions for both tunnels

B. An external VPN gateway resource with 2 interfaces, 2 Cloud Routers in the same region, a cloud HA VPN gateway with one tunnel from each interface to each external VPN gateway interface, and BGP sessions for both tunnels

C. An external VPN gateway resource with 4 interfaces, a Cloud Router in the same region, 2 cloud HA VPN gateway with one tunnel from each interface to each external VPN gateway interface, and BGP sessions for all 4 tunnels

D. An external VPN gateway resource with 4 interfaces, 2 Cloud Routers in the same region, 2 cloud HA VPN gateways with one tunnel from each interface to each external VPN gateway interface, and BGP sessions for all 4 tunnels

4.2 Configuring a site-to-site IPsec VPN

Courses

Networking in Google Cloud
- M13 Connectivity options
- M14 Cloud VPN

Networking in Google Cloud: Hybrid and Multicloud
- M1 Connectivity options
- M2 Cloud VPN

Skill Badge

Google Cloud

Network Performance and Optimization

Documentation

- VPC Network Peering overview
- Shared VPC overview
- Enabling multiple VPC networks to access the same VLAN attachment
- Cloud VPN overview
- Creating a Classic VPN using static routing
- Networks and tunnel routing | Cloud VPN
- HA VPN topologies
- Creating an HA VPN gateway to a peer VPN gateway

4.3 Diagnostic Question 08

You have an HA VPN gateway with 2 interfaces in active/active mode. You would like to reconfigure them to active/passive mode.

Select the simplest configuration change that will satisfy this requirement.

A. Remove the BGP session for one of the HA VPN tunnels.

B. Disable the BGP session for one of the HA VPN tunnels.

C. Update the base advertised route priorities for both of the HA VPN tunnels' BGP sessions.

D. Update the base advertised route priority for one of the HA VPN tunnel's BGP sessions.

4.3 Diagnostic Question 09

Cymbal Bank has a Cloud Router in a region; the VPC advertises some of its subnets. The VPC advertises none of the subnets in other regions. You require an update to advertise all subnets in all regions for that VPC. You also want to automatically advertise newly added subnets, as well as stop advertising removed subnets in the future.

Select the simplest configuration that will accomplish this goal.

A. Update the Cloud Router custom advertisements by advertising the IP ranges for all the subnets across all regions, then update the configured list whenever subnets are added or removed.

B. Check the dynamic routing mode of the VPC and update it to global if it is currently regional. Update the Cloud Router custom advertisements by advertising the IP ranges for all the subnets across all regions, then update the configured list whenever subnets are added or removed.

C. Check the dynamic routing mode of the VPC and update it to global if it is currently regional. Configure the Cloud Router to default advertisement mode.

D. Check the dynamic routing mode of the VPC and update it to regional if it is currently global. Configure the Cloud Router to default advertisement mode.

4.3 Diagnostic Question 10

Cymbal Bank would like to achieve 99.99% availability for their Dedicated Interconnect link from an on-premises network to their VPC.

Select the configuration that will achieve this.

A. 1 Cloud Router in one region with the VPC in regional dynamic routing mode

B. 2 Cloud Routers in one region, with the VPC in global dynamic routing mode

C. 2 Cloud Routers in 2 distinct regions, with the VPC in regional dynamic routing mode

D. 2 Cloud Routers in 2 distinct regions, with the VPC in global dynamic routing mode

4.3 Configuring Cloud Router

Courses

Networking in Google Cloud
- M14 Cloud VPN

Networking in Google Cloud: Hybrid and Multicloud
- M2 Cloud VPN

VPC Networking: Cloud HA-VPN

Skill Badge

Google Cloud

Network Performance and Optimization

Documentation

Cloud Router overview

Creating Cloud Routers

Establishing BGP sessions | Cloud Router

Updating the base advertised route priority | Cloud Router

Custom route advertisements introduction | Cloud Router

Advertising custom IP ranges | Cloud Router

Advertising specific VPC subnets | Cloud Router

Creating an HA VPN gateway to a peer VPN gateway

Establishing 99.99% availability for Dedicated Interconnect

Establishing 99.99% availability for Partner Interconnect

Establishing 99.9% availability for Dedicated Interconnect

Establishing 99.9% availability for Partner Interconnect

4.4 Diagnostic Question 11

Cymbal Bank has implemented a hub-and-spoke topology using Network Connectivity Center to interconnect its on-premises data centers and cloud-based workloads. The bank is experiencing performance degradation in application response times between its New York data center and a critical cloud-based application hosted in the us-central1 region.

Your task is to identify potential bottlenecks or configuration issues within the environment that could be causing the performance degradation.

Which specific step can you take to help identify the issues?

A. Analyze Cloud Load Balancing configuration and health checks associated with the application.

B. Evaluate the Network Connectivity Center hub's network performance metrics, such as latency and packet loss.

C. Verify the MTU size configuration of the VPN tunnels connecting the New York data center to the Network Connectivity Center hub.

D. Check for BGP routing inconsistencies between the Network Connectivity Center hub and the New York VPC spoke.

4.4 Configuring Network Connectivity Center

Courses

Networking in Google Cloud
- M14 Cloud VPN

Networking in Google Cloud: Hybrid and Multicloud
- M2 Cloud VPN

Documentation

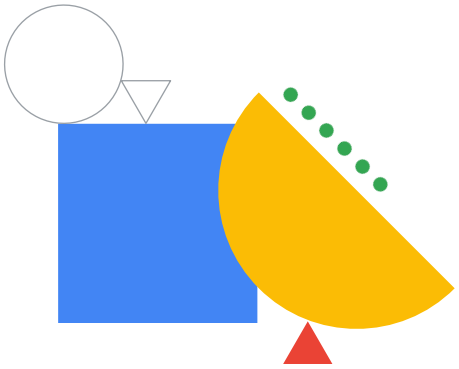
Network Connectivity Center overview | Google Cloud

Router appliance overview | Network Connectivity Center | Google Cloud

Router appliance overview | Network Connectivity Center | Google Cloud

Create router appliance instances | Network Connectivity Center | Google Cloud

Google Cloud



Section 5: Managing, monitoring, and troubleshooting network operations

5.1 Diagnostic Question 01

Cymbal Bank needs to log all cache hits and misses for their static assets served from Cloud CDN via an Application Load Balancer backend bucket.

What should you do?

A. Enable logging on the backend bucket and configure logging sample rate to 1.0.

B. Use the default behavior, no configuration required.

C. Enable logging on the backend bucket.

D. Configure the logging sample rate on the backend bucket to 1.0.

5.1 Diagnostic Question 02

You are designing a monitoring alert to notify you when a Cloud VPN tunnel approaches the limits for bandwidth.

Select the metrics that would be important to include in the alerting policies.

A. vpn.googleapis.com/network/sent_bytes_count,
vpn.googleapis.com/network/received_bytes_count,
vpn.googleapis.com/network/sent_packets_count,
vpn.googleapis.com/network/received_packets_count

B. vpn.googleapis.com/network/dropped_received_packets_count,
vpn.googleapis.com/network/network/dropped_sent_packets_count

C. vpn.googleapis.com/network/sent_bytes_count,
vpn.googleapis.com/network/received_bytes_count

D. vpn.googleapis.com/network/sent_packets_count,
vpn.googleapis.com/network/received_packets_count,
vpn.googleapis.com/network/dropped_received_packets_count,
vpn.googleapis.com/network/network/dropped_sent_packets_count

5.1 Diagnostic Question 03

Cymbal Bank's network team wants to track and analyze detailed logs of all API calls made to their Google Cloud resources, including timestamps, user identities, and specific actions taken.

Which Google Cloud service is the most appropriate choice for Cymbal Bank's network team to achieve this goal?

A. Cloud Audit Logs

B. Cloud Logging

C. VPC Flow Logs

D. Cloud Monitoring

5.1 Logging and monitoring with Google Cloud Observability

Courses

Networking in Google Cloud
- M3 Network Monitoring and Logging
- M12: Caching and Optimizing Load Balancing

Networking in Google Cloud: Fundamentals
- M3 Network Monitoring and Logging

Networking in Google Cloud: Load Balancing
- M2: Caching and Optimizing Load Balancing

Skill Badge

Google Cloud

Network Performance and Optimization

Documentation

Global external Application Load Balancer logging and monitoring

View logs and metrics | Cloud Router

Logs and metrics | Cloud NAT

Logs and metrics | Cloud VPN

VPC Service Controls audit logging

Google Cloud Armor audit logging information

Using request logging

Monitor connections | Cloud Interconnect

Monitoring Google Cloud Armor security policies

Google Cloud metrics | Cloud Monitoring

5.2 Diagnostic Question 04

You are using VPC Flow Logs to analyze traffic arriving at a subnet. You need to capture approximately 10% of the traffic and determine how much traffic originates from outside the subnet. VPC Flow Logs has already been enabled for the subnet. You want to use the least expensive process.

How should you configure VPC Flow Logs?

A. Configure them with a sampling rate of 0.1 and a filter expression for the connection source and destination IP within the IP range of the subnet.

B. Configure them with a sampling rate of 1.0 and a filter expression for the connection source and destination IP within the IP range of the subnet.

C. Configure them with a sampling rate of 0.1 and a filter expression for the connection destination IP within the IP range of the subnet.

D. Configure them with a sampling rate of 1.0 and a filter expression for the connection destination IP within the IP range of the subnet.

5.2 Diagnostic Question 05

Cymbal Bank has configured a Classic VPN with a policy-based tunnel to connect to a branch office with an older VPN device that does not support BGP. You have completed the configuration of the office VPN and the logs and monitoring suggest that the tunnel is up and functioning correctly. You find when testing with ping and traceroute that you can reach some VMs but not others in the VPC across the tunnel from the office. You can reach some servers but not others in the office from VMs in the VPC. You have verified the firewall configurations in both environments and determined that is not the cause of the problem.

What is the next troubleshooting step you should attempt?

A. Investigate the Cloud Router configuration for advertised subnets.

B. Investigate the Cloud Router BGP session status.

C. Investigate the configuration of the local and remote traffic selectors in the Classic VPN tunnel and office VPN configuration.

D. Search the Classic VPN tunnel logs for IKE events indicating a problem.

5.2 Diagnostic Question 06

You are debugging a Layer 2 Partner Interconnect connection that is indicating a failure to create a BGP session in the Cloud Router for the associated VLAN attachments.

Select the most likely cause to investigate when troubleshooting this issue.

A. Check the ASN configuration of the on-premises router and the Cloud Router.

B. Check the BGP keepalive timer configuration of the Cloud Router.

C. Check the route advertisement configuration of the Cloud Router.

D. Check the route configuration of the VPC the Cloud Router is in.

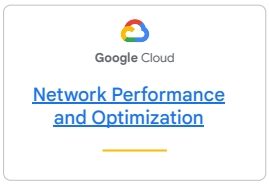
5.2 Maintaining and troubleshooting connectivity issues

Courses

Networking in Google Cloud
- M3 Network Monitoring and Logging

Networking in Google Cloud: Fundamentals
- M3 Network Monitoring and Logging

Skill Badge



Documentation

VPC Flow Logs overview
Using VPC Flow Logs
Viewing logs and metrics | Cloud VPN
Troubleshooting | Cloud VPN
Viewing Cloud Router logs and metrics
Troubleshooting | Cloud Router
Troubleshooting | Cloud Interconnect

5.3 Diagnostic Question 07

You are trying to debug a connectivity issue between VMs in the same VPC using internal IP addresses. The issue began immediately after configuring routes and firewall rules.

What should you do to troubleshoot the problem?

A. Disable firewall rules one by one in all combinations to determine the problem.

B. Remove static routes one by one in all combinations to determine the problem.

C. Review the packet loss statistics in the Network Intelligence Center performance dashboard.

D. Use Connectivity Tests to determine the connectivity problem.

5.3 Diagnostic Question 08

You are a network administrator responsible for monitoring and troubleshooting networking issues in Cymbal Bank's Google Cloud environment. You want to use Network Intelligence Center to identify and resolve common networking problems.

Which of the following capabilities does Network Intelligence Center provide to help you monitor and troubleshoot common networking issues? (Select TWO correct options.)

A. Real-time network topology visualization

B. Automated network configuration management

C. Flow logs analysis for traffic visibility

D. Predictive network failure alerts

E. Firewall rule recommendations

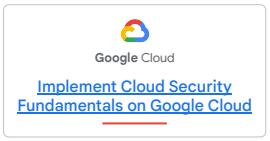
5.3 Using Network Intelligence Center to monitor and troubleshoot common networking issues

Courses

Networking in Google Cloud
- M3 Network Monitoring and Logging

Networking in Google Cloud: Fundamentals
- M3 Network Monitoring and Logging

Skill Badges



Documentation

- Calculating network throughput
- Using netperf and ping to measure network latency
- Performance Dashboard overview
- Network Topology metrics reference
- Google Cloud Performance Kit Benchmarker
- Routes overview | VPC
- Troubleshooting VM-VM connectivity with internal IP addresses | VPC
- Troubleshooting | Cloud Router
- Connectivity Tests overview
- Performance Dashboard overview
- Firewall Insights overview
- Network Topology overview
- Network Topology metrics reference
- Connectivity Tests overview
- Network Analyzer overview

Plan time to prepare

When will you take the exam?

How many weeks do you have to prepare?

How many hours will you spend preparing for the exam each week?

How many total hours will you prepare?

Example 6-week plan

Week 1	Week 2	Week 3	Week 4	Week 5	Week 6
Google Cloud Fundamentals: Core Infrastructure	Networking in Google Cloud: Fundamentals	Networking in Google Cloud: Network Architecture	Networking in Google Cloud: Hybrid and Multicloud	Observability in Google Cloud	Sample questions
Networking Fundamentals in Google Cloud Skill Badge	Networking in Google Cloud: Routing and Addressing	Networking in Google Cloud: Network Security	Logging and Monitoring in Google Cloud	Network Performance and Optimization Skill Badge	Review documentation
Set Up an App Dev Environment on Google Cloud Skill Badge	Build a Secure Google Cloud Network Skill Badge	Implement Load Balancing on Compute Engine Skill Badge	Configure Google Kubernetes Engine Networking Skill Badge	Implement Cloud Security Fundamentals on Google Cloud Skill Badge	

Weekly study plan

Now, consider what you've learned about your knowledge and skills through the diagnostic questions in this course. You should have a better understanding of what areas you need to focus on and what resources are available.

Use the template that follows to plan your study goals for each week. Consider:

- What exam guide section(s) or topic area(s) will you focus on?
- What courses (or specific modules) will help you learn more?
- What Skill Badges or labs will you work on for hands-on practice?
- What documentation links will you review?
- What additional resources will you use - such as sample questions?

You may do some or all of these study activities each week.

Duplicate the weekly template for the number of weeks in your individual preparation journey.

Weekly study template (example)

Area(s) of focus:	Configuring VPCs
Courses/modules to complete:	Networking in Google Cloud: Fundamentals Module 1, Module 2 Networking in Google Cloud: Network Security Module 2
Skill Badges/labs to complete:	Implement Cloud Security Fundamentals on Google Cloud
Documentation to review:	VPC network overview Using VPC networks VPC firewall rules overview Using firewall rules | VPC
Additional study:	Sample questions 1-3

Weekly study template

Area(s) of focus:	
Courses/modules to complete:	
Skill Badges/labs to complete:	
Documentation to review:	
Additional study:	