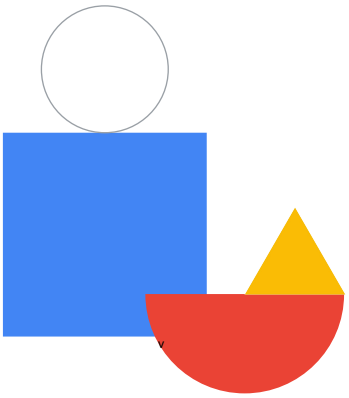
Google Cloud

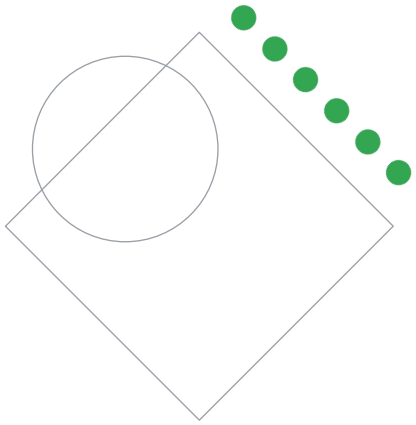


Preparing for Your Professional Cloud Network Engineer Journey

Module 2: Implementing Virtual Private Cloud (VPC) networks

Welcome to Module 2: Implementing Virtual Private Cloud (VPC) networks.

Review and study planning

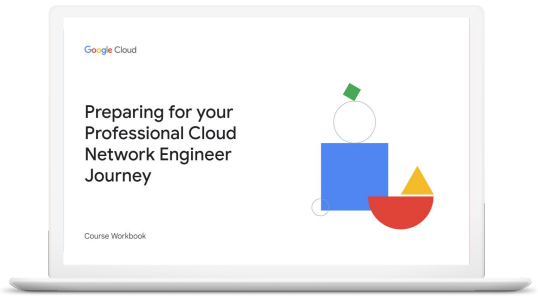


Google Cloud

You'll now review the diagnostic questions and your answers to help you identify what to include in your study plan.

Your study plan:

Implementing Virtual Private Cloud (VPC) networks



2.1	Configuring VPCs
2.2	Configuring VPC routing
2.3	Configuring Network Connectivity Center
2.4	Configuring and maintaining Google Kubernetes Engine clusters
2.5	Configuring and managing Cloud Next Generation Firewall (NGFW) rules

Google Cloud

The diagnostic questions align with these objectives of this exam section. Use the PDF resource that follows to review the questions and how you answered them. Pay specific attention to the rationale for both the correct and incorrect answers. Use the resources detailed under Where to look and Content mapping to build a study plan that meets your learning needs.

2.1 Configuring VPCs

Considerations include:

- Creating Google Cloud VPC resources (e.g., networks, subnets, firewall rules/policy)
- Configuring VPC Network Peering
- Creating a Shared VPC network and sharing subnets with other projects
- Configuring API access to Google services (e.g., Private Google Access, public interfaces)
- Expanding VPC subnet ranges after creation

Google Cloud

A Professional Cloud Network Engineer should be able to take a high-level design of networks and distribution of resources within them to create, connect, and configure the associated networking infrastructure. You'll need to consider the distribution of resources across regions and zones and how to satisfy availability, capacity, performance, and cost requirements. You should be able to define the details of communication across resources or between resources and external environments.

You explored these considerations in the diagnostic questions. Question 1 covered subnet configuration, primary and secondary IP ranges, expanding subnets, routing rules, and firewalls. Question 2 covered Shared VPC and VPC Peering, including configuration and knowing when to use them.

To answer these questions, you should be comfortable with all of the considerations listed on the slide.

2.1 Diagnostic Question 01 Discussion

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.

Feedback:
A. Incorrect. Creating a new subnet with that range would cause overlap with the old ranges.
B. Incorrect. This forces all VMs from both subnets to be deleted and recreated, which does not minimize interruption.
*C. Correct! This option minimizes interruption by only moving VMs from the subnet to be deleted while expanding the other subnet, which does not require VMs to be recreated.
D. Incorrect. You can't change the primary range prefix of an existing subnet because only expansion is possible.

Where to look:
https://cloud.google.com/vpc/docs/vpc
https://cloud.google.com/vpc/docs/using-vpc
https://cloud.google.com/vpc/docs/firewalls
https://cloud.google.com/vpc/docs/using-firewalls

Content mapping:

- ILT course: **Networking in Google Cloud**
  - M1 VPC Networking Fundamentals
  - M9 Controlling Access to VPC Networks

- On-demand course: **Networking in Google Cloud: Fundamentals**
  - M1 VPC Networking Fundamentals

- On-demand course: **Networking in Google Cloud: Network Security**
  - M2 Controlling Access to VPC Networks

- Skill badges:
  - Networking Fundamentals in Google Cloud
  - Build a Secure Google Cloud Network

Summary:
When configuring VPC networks and their subnetworks, you can expand the primary range of a subnet (to max /16 size in auto networks or to the size supported by the IP block in custom networks) as long as the expansion does not introduce overlap to other existing subnets. When doing such expansion, any firewall rules depending on the older range should be updated.

Secondary ranges cannot be expanded or changed and must be deleted and recreated. Secondary ranges are used by an alias IP allowing secondary internal IP addresses to be assigned to the VM, typically for container or pod networking. Deleting a subnet first requires deleting all VMs in that subnet.

Many traffic control scenarios can be accomplished leaving the default routes and adding, removing, or changing only the firewall rules. You can set multiple rules to be applied in priority order - but remember to account for the implicit deny all ingress and allow all egress rules at lowest priority.

2.1 Diagnostic Question 02 Discussion

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) 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).

Feedback:
A. Incorrect. VPC peering is not transitive (“V1 to V2 and V2 to V3” does not provide connectivity between V1 and V3). Also, this option doesn’t satisfy the requirement to have centralized/consolidated network billing, administration, and access control for Cymbal project networking.
B. Incorrect. VPC peering is not transitive (“V6 peered to V4 and V4 peered to V5” does not provide connectivity between V6 and V5).
C. Incorrect. Shared VPC cannot work across organizations (only for projects within the same organization).
*D. Correct! This option satisfies the requirements and provides connectivity between VMs of all the projects.

Where to look:
https://cloud.google.com/vpc/docs/vpc-peering
https://cloud.google.com/vpc/docs/using-vpc-peering
https://cloud.google.com/vpc/docs/shared-vpc
https://cloud.google.com/vpc/docs/provisioning-shared-vpc

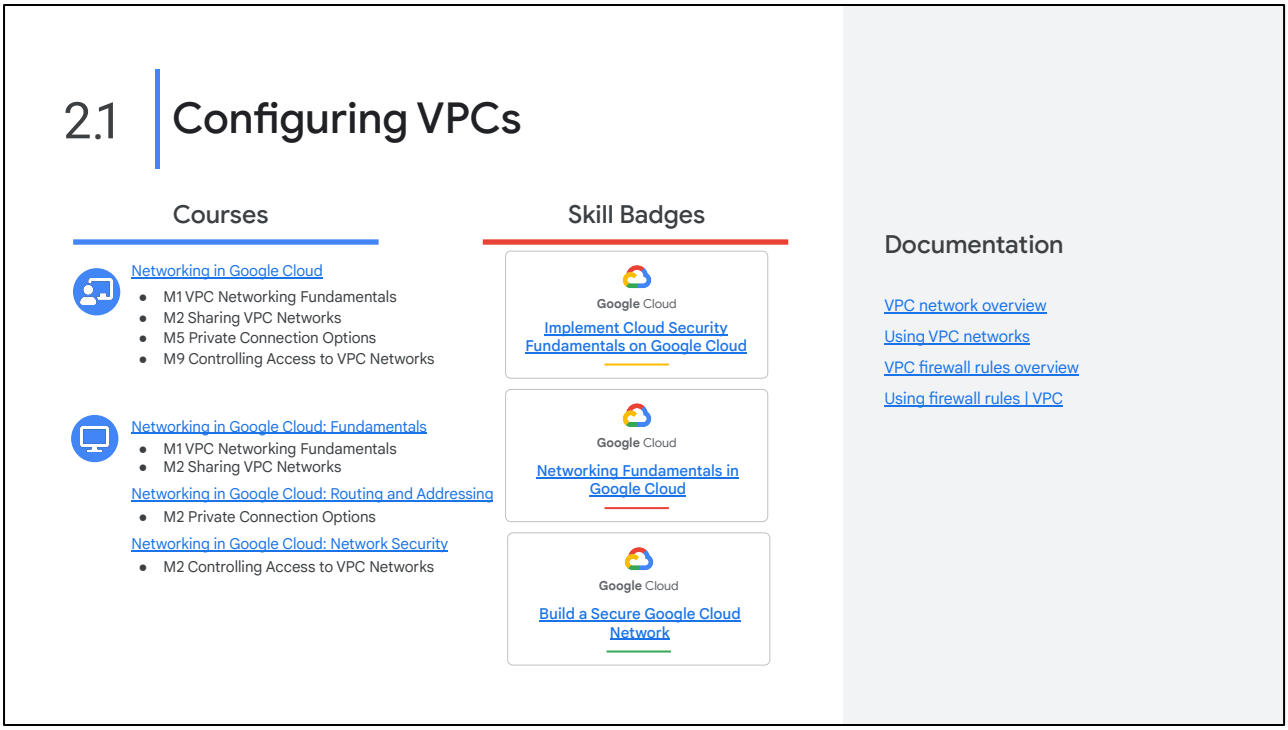
Content mapping:
- ILT course: **Networking in Google Cloud**
  - M2 Sharing VPC Networks
  - M5 Private Connection Options
- On-demand course: **Networking in Google Cloud: Fundamentals**

    - M2 Sharing VPC Networks

- On-demand course: **Networking in Google Cloud: Routing and Addressing**
    - M2 Private Connection Options

- Skill badges:
    - Networking Fundamentals in Google Cloud
    - Implement Cloud Security Fundamentals on Google Cloud

Summary:
Shared VPC is a centralized networking model (for billing, administration, and access control) whereas VPC peering is a decentralized approach. VPC peering can work across organizations whereas Shared VPC can only work within organizations. VPC peering does not support transitive peering and requires any two connected VPCs to be directly peered.



Let's consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Fundamentals (On-demand)
Networking in Google Cloud: Routing and Addressing (On-demand)
Networking in Google Cloud: Network Security (On-demand)

Implement Cloud Security Fundamentals on Google Cloud
Networking Fundamentals in Google Cloud
Build a Secure Google Cloud Network

https://cloud.google.com/vpc/docs/vpc
https://cloud.google.com/vpc/docs/using-vpc
https://cloud.google.com/vpc/docs/firewalls
https://cloud.google.com/vpc/docs/using-firewalls

2.2 Configuring VPC routing

Considerations include:

- Setting up static and dynamic routing
- Configuring global or regional dynamic routing
- Implementing routing using network tags and priority
- Implementing an internal load balancer as a next hop
- Configuring custom route import/export over VPC Network Peering
- Configuring Policy-based Routing

Google Cloud

A Professional Cloud Network Engineer should be able to define the necessary routing infrastructure and configuration to support the communication requirements of the workloads in the VPCs. Considerations include those shown on the slide, including type of routing, routing policies, importing and exchanging custom routes over VPC network peering.

You explored these considerations in the diagnostic questions. Question 3 tested your knowledge of VPN routing options such as policy- versus route-based and global versus regional. Question 4 tested your ability to configure routing rules for custom routing scenarios.

2.2 Diagnostic Question 03 Discussion

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.

Feedback:
A. Incorrect. The second office VPN gateway (close to us-east1) does not support BGP.
B. Incorrect. This option does not provide the highest availability. The Classic VPN used to connect the second office to the VPC in the us-east1 region has lower availability. And when it fails, the traffic would not reroute to use the other VPN connection automatically because the VPC is configured for regional dynamic routing mode.
C. Incorrect. The second office VPN gateway (close to us-east1) does not support BGP.
*D. Correct! This option provides the highest availability. Classic VPN used to connect the second office to the VPC in us-east1 has lower availability, but when it fails the traffic will automatically reroute to use the other HA VPN connection.

Where to look:
https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview
https://cloud.google.com/network-connectivity/docs/vpn/concepts/best-practices
https://cloud.google.com/network-connectivity/docs/vpn/concepts/topologies
https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies
https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-ha-vpn
https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-ha-vpn2
https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns
https://cloud.google.com/network-connectivity/docs/vpn/concepts/choosing-networks-routing

https://cloud.google.com/network-connectivity/docs/router/concepts/overview

Content mapping:

- ILT course: **Networking in Google Cloud**
  - M13 Connectivity Options
  - M14 Cloud VPN

- On-demand course: **Networking in Google Cloud: Hybrid and Multicloud**
  - M1 Connectivity Options
  - M2 Cloud VPN

- Skill badge: Network Performance and Optimization

Summary:
HA VPN only supports dynamic routing with BGP and can't be used if the peer on-premises VPN gateway does not support BGP. Classic VPN supports static routing, either route-based or policy-based. Use Classic VPN when the on-premises VPN gateway does not support BGP.

HA VPN provides 99.99% availability; Classic VPN only supports 99.9% availability. HA VPN is the recommended approach whenever the on-premises VPN gateway supports BGP.

Dynamic routing requires a Cloud Router. Dynamic routing is simpler to configure and maintain than static routing because route changes in either connected network can be discovered and advertised automatically. The Dynamic routing mode of the VPC determines whether Cloud Routers will use regional or global dynamic routing or dynamic routing. A single VPN connection can provide connectivity across all subnets and regions within a VPC when the VPC is in global dynamic routing mode. However, the average latency will not be as low as if there are separate Cloud VPN gateways and Cloud Routers per region.

2.2 Diagnostic Question 04 Discussion

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.

Feedback:
A. Incorrect. You can't create a new custom route to the 0.0.0.0/0 destination until you first delete the system-generated default route (which goes to that same destination).
B. Incorrect. You must enable IP forwarding in a VM to allow it to proxy egress traffic.
C. Incorrect. You can't create a new custom route to the 0.0.0.0/0 destination until you first delete the system-generated default route (which goes to that same destination).
*D. Correct! This is the minimal set of steps to configure this routing scenario.

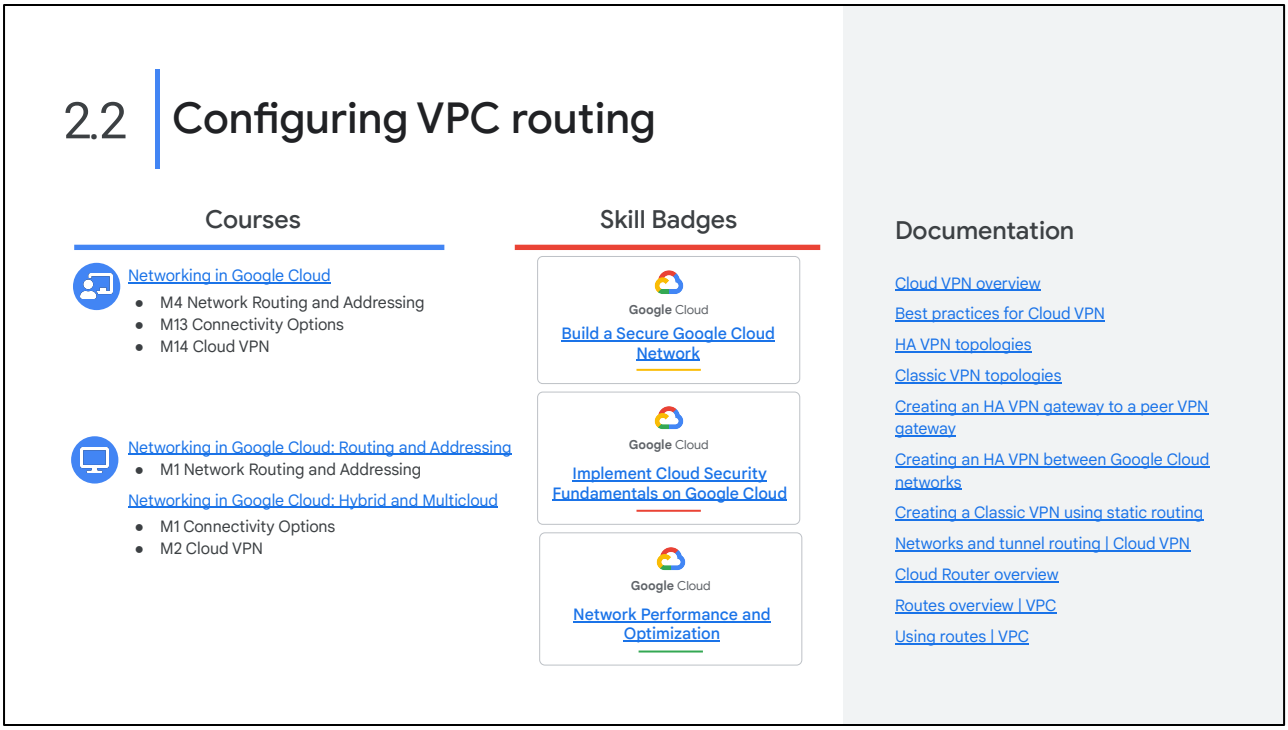
Where to look:
https://cloud.google.com/vpc/docs/routes
https://cloud.google.com/vpc/docs/using-routes

Content mapping:

- Partial coverage in ILT course: **Networking in Google Cloud**
  - M4 Network Routing and Addressing
- Partial coverage in on-demand course: **Networking in Google Cloud: Routing and Addressing**
  - M1 Network Routing and Addressing
- Skill badges:
  - Build a Secure Google Cloud Network
  - Implement Cloud Security Fundamentals on Google Cloud

- Network Performance and Optimization

Summary:
Most standard network routing can be accomplished using the default created routes. In some scenarios, traffic must be forwarded through a NAT or Proxy instance, or routed through an intermediary different than the destination IP address. This can be accomplished by creating custom routes. When creating a custom route, you can specify a destination IP address or range and the next hop instance, load balancer, IP address, internet gateway, or VPN gateway. You can limit which VMs would use a custom route by adding a tag to the custom route that matches a tag on the appropriate VMs.



Let's consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Routing and Addressing (On-demand)
Networking in Google Cloud: Hybrid and Multicloud (On-demand)

Build a Secure Google Cloud Network (Skill badge)
Implement Cloud Security Fundamentals on Google Cloud (Skill badge)
Network Performance and Optimization (Skill badge)

https://cloud.google.com/network-connectivity/docs/vpn/concepts/overview
https://cloud.google.com/network-connectivity/docs/vpn/concepts/best-practices
https://cloud.google.com/network-connectivity/docs/vpn/concepts/topologies
https://cloud.google.com/network-connectivity/docs/vpn/concepts/classic-topologies
https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-ha-vpn
https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-ha-vpn2
https://cloud.google.com/network-connectivity/docs/vpn/how-to/creating-static-vpns

https://cloud.google.com/network-connectivity/docs/vpn/concepts/choosing-networks-routing
https://cloud.google.com/network-connectivity/docs/router/concepts/overview
https://cloud.google.com/vpc/docs/routes
https://cloud.google.com/vpc/docs/using-routes

2.3 Configuring Network Connectivity Center

Considerations include:

- Managing VPC topology (e.g., star topology, hub and spoke, mesh topology).
- Implementing Private NAT

Google Cloud

A Professional Cloud Network Engineer should be able to effectively design, implement, and manage network connectivity using Network Connectivity Center. Considerations include those shown on the slide and include an understanding of topology and design principles, security, cost optimization, and operational considerations.

You explored these considerations in the diagnostic question. Question 5 tested your knowledge of Google Cloud Networking, and Network design and implementation.

2.3 Diagnostic Question 05 Discussion

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.

Feedback:
A. Incorrect. While a hybrid cloud approach can be beneficial, it requires careful planning and execution, and might not directly address the core challenges of network management and security.
B. Incorrect. While a zero-trust approach is crucial for security, it's not a complete solution for network performance and scalability.
*C. Correct! This option provides a comprehensive approach to address the bank's challenges by offering centralized management, security, and scalability.
D. Incorrect. While Cloud Interconnect can enhance connectivity, it's not the best fit for connecting multiple remote branches to a central cloud environment and doesn't address the broader network management challenges.

Where to look:
https://cloud.google.com/network-connectivity/docs/network-connectivity-center/concepts/overview
https://cloud.google.com/nat/docs/about-private-nat-for-ncc
https://cloud.google.com/nat/docs/set-up-private-nat

Content mapping:

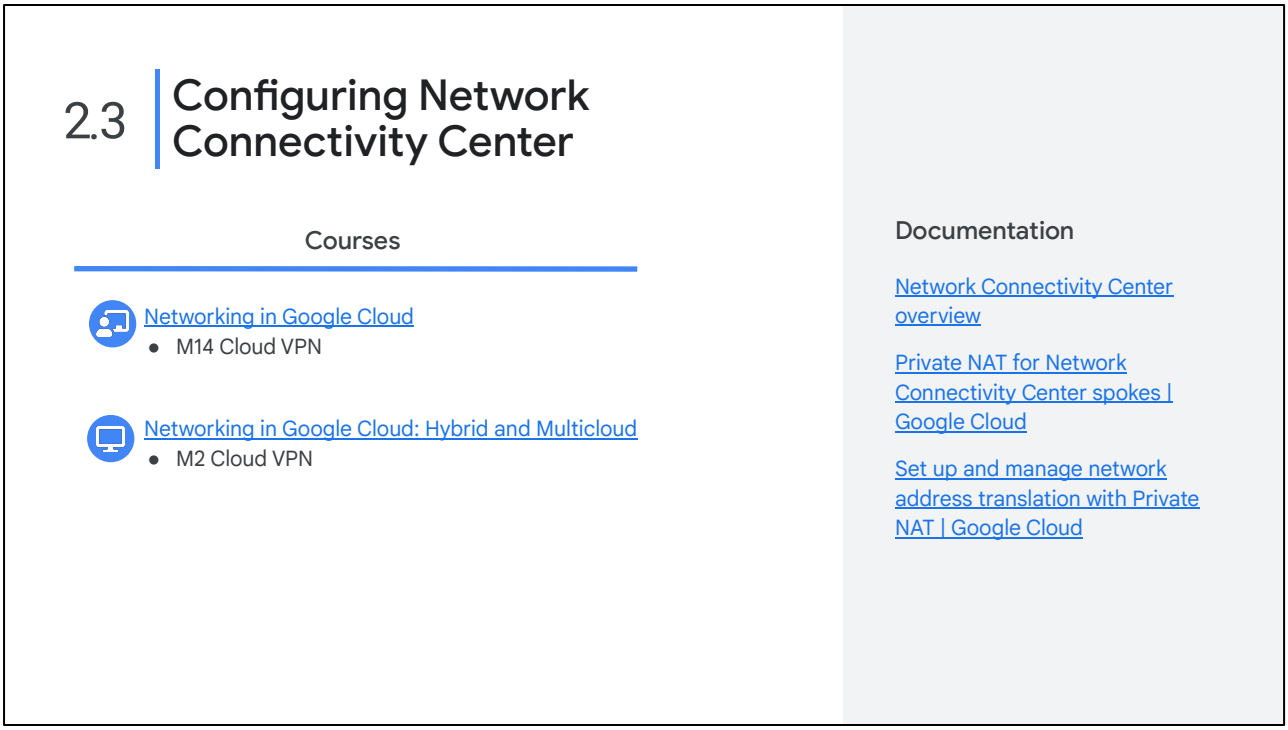
- ILT course: **Networking in Google Cloud**
  - M14 Cloud VPN

- On-demand course: **Networking in Google Cloud: Hybrid and Multicloud**
  - M2 Cloud VPN

Summary:

Network Connectivity Center with Cloud VPN is the optimal solution for Cymbal Bank due to its comprehensive approach to network management. By centralizing network management, it simplifies operations and reduces complexity. Additionally, it ensures robust security through secure VPN connections, protecting sensitive customer data. The solution's scalability allows for easy expansion as the bank grows, while Cloud VPN optimizes network performance.

In comparison, other options like hybrid cloud networking and zero-trust security, while valuable, do not directly address the core challenges of network management, connectivity, and scalability as effectively as Network Connectivity Center with Cloud VPN. This solution provides a holistic approach that meets Cymbal Bank's specific needs.



Let's consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic question we just reviewed are covered in this module and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Hybrid and Multicloud (On-demand)

https://cloud.google.com/network-connectivity/docs/network-connectivity-center/concepts/overview
https://cloud.google.com/nat/docs/about-private-nat-for-ncc
https://cloud.google.com/nat/docs/set-up-private-nat

2.4 Configuring and maintaining Google Kubernetes Engine clusters

Considerations include:

- Creating VPC-native clusters using alias IPs
- Setting up clusters with Shared VPC
- Configuring private clusters and private control plane endpoints
- Adding authorized networks for cluster control plane endpoints
- Configuring Service Mesh.
- Enabling GKE Dataplane V2.
- Configuring source NAT (SNAT) and IP Masquerade policies
- Creating GKE network policies
- Configuring Pod ranges and service ranges, and deploying additional Pod ranges for GKE clusters

Google Cloud

A Professional Cloud Network Engineer will be responsible for configuring all the networking related details of Kubernetes Engine clusters. Some considerations are noted on the slide; for example, VPC-native clusters using alias IPs, clusters with Shared VPC, and Creating Kubernetes network policies.

You explored these considerations in the diagnostic questions. Question 5 tested your knowledge of pod and service IP ranges for GKE networking. Question 6 tested your ability to work with specialized GKE networking scenarios.

To answer these questions, you should be comfortable with all of the considerations listed on this slide.

2.4 Diagnostic Question 06 Discussion

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.

Feedback:
A. Incorrect. Expansion of the subnet is unnecessary because there are enough IP addresses for sufficient nodes to support 200,000 pods. The secondary ranges can be specified when creating the cluster. Also, the pod range is not large enough for 200,000 pods (requires /13 size) because each pod requires one IP address.
B. Incorrect. Secondary ranges can be created automatically when the GKE cluster is created and don't require manual creation beforehand. Also, the service range is larger than necessary to support 30,000 service (/17 would suffice) because each pod requires one IP address.
C. Incorrect. The pod range is not large enough for 200,000 pods (requires /13 size) because each pod requires one IP address.
*D. Correct! This is the minimal configuration with the smallest possible ranges because each pod and service requires one IP address..

Where to look:
https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters
https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips
https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips
https://cloud.google.com/kubernetes-engine/docs/how-to/flexible-pod-cidr

Content mapping:
- On-demand course: **Configure Google Kubernetes Engine Networking**
  - M1 GKE Networking Overview

- Highly recommend reviewing documentation.
- Minor coverage in skill badge: Implement Cloud Security Fundamentals on Google Cloud.

Summary:
For VPC-native clusters, secondary subnet ranges are used for pod and service IP ranges. You can either pre-create the secondary ranges or simply specify them when creating the cluster. Each node will support up to 110 pods. The primary IP range needs to be large enough that when the number of nodes is multiplied by 110, the supported number of pods will be sufficient. The size of the pod range also needs to be large enough to provide one IP address per pod for the maximum number of pods. The service range should be large enough to provide one IP address for the maximum number of services.

2.4 Diagnostic Question 07 Discussion

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.serviceaccount.com service account (where serviceProjectNumber is the project number of the service project).

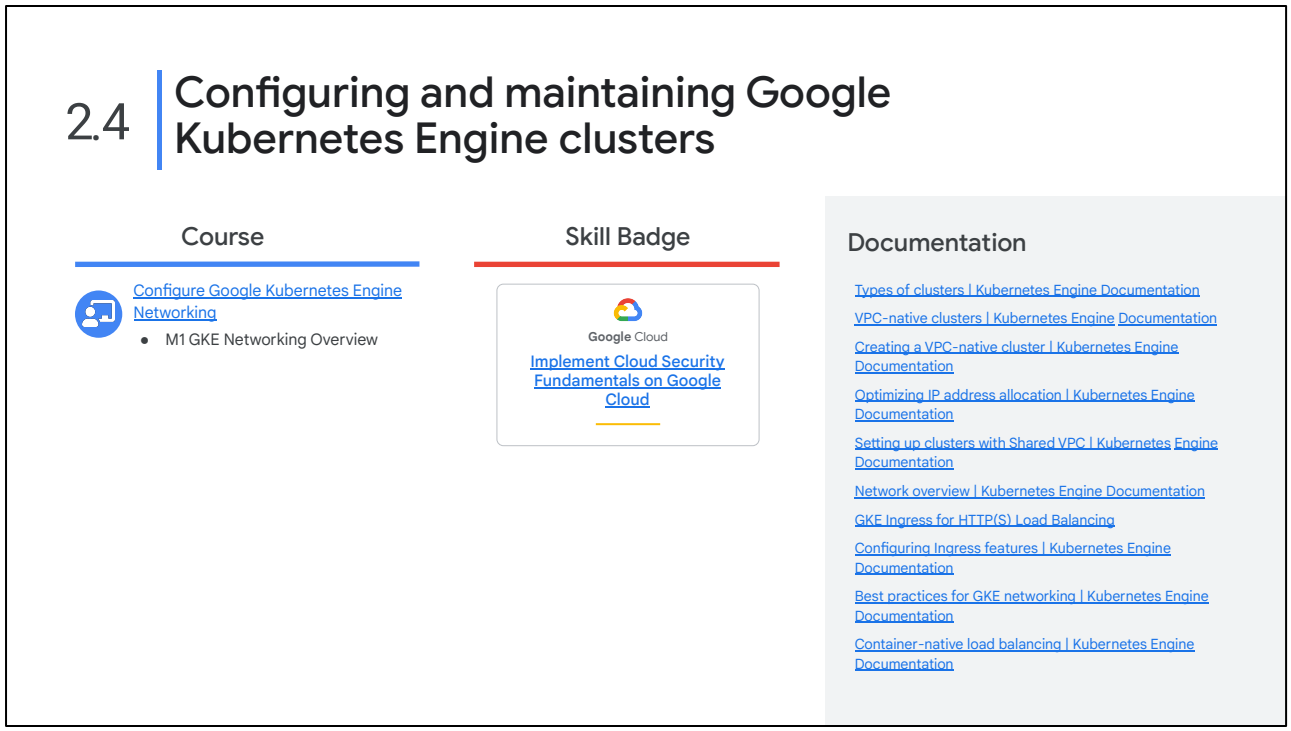
Feedback:
A. Incorrect. This option is missing a necessary role binding.
B. Incorrect. This option is missing a necessary role binding.
C. Incorrect. This option is not least privileged access (it provides access to the entire VPC when only the subnet hosting the GKE cluster is necessary).
*D. Correct! This is the least privilege option.

Where to look:
https://cloud.google.com/kubernetes-engine/docs/how-to/cluster-shared-vpc
https://cloud.google.com/kubernetes-engine/docs/concepts/network-overview
https://cloud.google.com/kubernetes-engine/docs/concepts/ingress
https://cloud.google.com/kubernetes-engine/docs/how-to/ingress-features
https://cloud.google.com/kubernetes-engine/docs/best-practices/networking
https://cloud.google.com/kubernetes-engine/docs/concepts/container-native-load-balancing

Content mapping:
Not in current learning path, please refer to documentation.

Summary:
When running GKE clusters in a Shared VPC, some extra IAM role bindings must be granted to the Kubernetes Engine service agent to let the GKE cluster create the necessary networking resources. It requires the Compute Network User role for the Shared VPC subnet of the GKE cluster, as well as the Host Service Agent User for

the Shared VPC host project.



Let's consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in this Skill Badge and in this documentation. **Reviewing the documentation is highly recommended!** You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Configure Google Kubernetes Engine Networking (on-demand)

Implement Cloud Security Fundamentals on Google Cloud (Skill badge)

https://cloud.google.com/kubernetes-engine/docs/concepts/types-of-clusters
https://cloud.google.com/kubernetes-engine/docs/concepts/alias-ips
https://cloud.google.com/kubernetes-engine/docs/how-to/alias-ips
https://cloud.google.com/kubernetes-engine/docs/how-to/flexible-pod-cidr
https://cloud.google.com/kubernetes-engine/docs/how-to/cluster-shared-vpc
https://cloud.google.com/kubernetes-engine/docs/concepts/network-overview
https://cloud.google.com/kubernetes-engine/docs/concepts/ingress
https://cloud.google.com/kubernetes-engine/docs/how-to/ingress-features
https://cloud.google.com/kubernetes-engine/docs/best-practices/networking
https://cloud.google.com/kubernetes-engine/docs/concepts/container-native-load-bala

ncing

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

Considerations include:

- Creating the firewall rules and regional/global policies
- Mapping target network tags, service accounts, and secure tags
- Migrating from firewall rules to firewall policies
- Configuring firewall rule criteria (e.g. rule priority, network protocols, ingress and egress rules)
- Configuring Firewall Rules Logging
- Configuring hierarchical firewall policies
- Configuring the intrusion prevention service (IPS)
- Implementing fully qualified domain name (FQDN) firewall objects

Google Cloud

The Professional Cloud Network Engineer uses firewall rules as the primary mechanism of traffic control with the VPCs and should be able to configure them to support all common workload communication scenarios. Considerations include target network tags and service accounts, rule priority, and network protocols.

You explored these considerations in the diagnostic questions. Question 7 tested your ability to configure firewall rules. Question 8 tested your ability to troubleshoot connectivity issues using firewall logging and insights.

2.5 Diagnostic Question 08 Discussion

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.

Feedback:
*A. Correct! This option is as simple as the others but provides better security: service accounts have tighter access control than network tags.
B. Incorrect. This option is slightly less secure than option A: service accounts have tighter access control than network tags.
C. Incorrect. This option is significantly less secure than option A. It would allow requests into the microservices from any other workloads deployed in the same subnet, using the same ports as the intended microservices.
D. Incorrect. This is significantly less secure than option A because it would allow requests into the microservices from any other workloads deployed in the same subnet using the same ports as the intended microservices.

Where to look:
https://cloud.google.com/vpc/docs/firewalls
https://cloud.google.com/vpc/docs/using-firewalls

Content mapping:
- ILT course: **Networking in Google Cloud**
  - M9 Controlling Access to VPC Networks
  - M11 Hybrid Load Balancing and Traffic Management

- On-demand course: **Networking in Google Cloud: Network Security**
  - M2 Controlling Access to VPC Networks

- On-demand course: **Networking in Google Cloud: Load Balancing**
    - M1 Hybrid Load Balancing and Traffic Management

- Skill badges:
    - Build a Secure Google Cloud Network
    - Implement Cloud Security Fundamentals on Google Cloud
    - Network Performance and Optimization
    - Networking Fundamentals in Google Cloud

Summary:
Firewall rules can be assigned to operate on all instances in a VPC. You can also assign them to specific VMs using source or destination IP addresses or IP ranges. You can also assign firewall rules using source and target service accounts or tags. In general using source and target service accounts is the recommended approach and provides the best security.

2.5 Diagnostic Question 09 Discussion

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 or Legacy Logs Viewer 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).

Feedback:
A. Incorrect. This approach will not work if the traffic is being blocked by the implicit deny all ingress rule (i.e., there is no appropriate allow rule that is allowing the requests to ingress VM2).
*B. Correct! This is the only approach among the options that will detect the incorrectly configured rule whether it is a missing or incorrect ingress allow or a incorrect egress deny rule.
C. Incorrect. This approach will not work if the traffic is being blocked by some deny egress rule at VM1.
D. Incorrect. This approach will not work if the traffic is being blocked by some deny egress rule at VM1.

Where to look:
https://cloud.google.com/vpc/docs/firewall-rules-logging
https://cloud.google.com/vpc/docs/using-firewall-rules-logging
https://cloud.google.com/network-intelligence-center/docs/firewall-insights/how-to/using-firewall-insights
https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/overview

Content mapping (Partial coverage in Networking in Google Cloud):

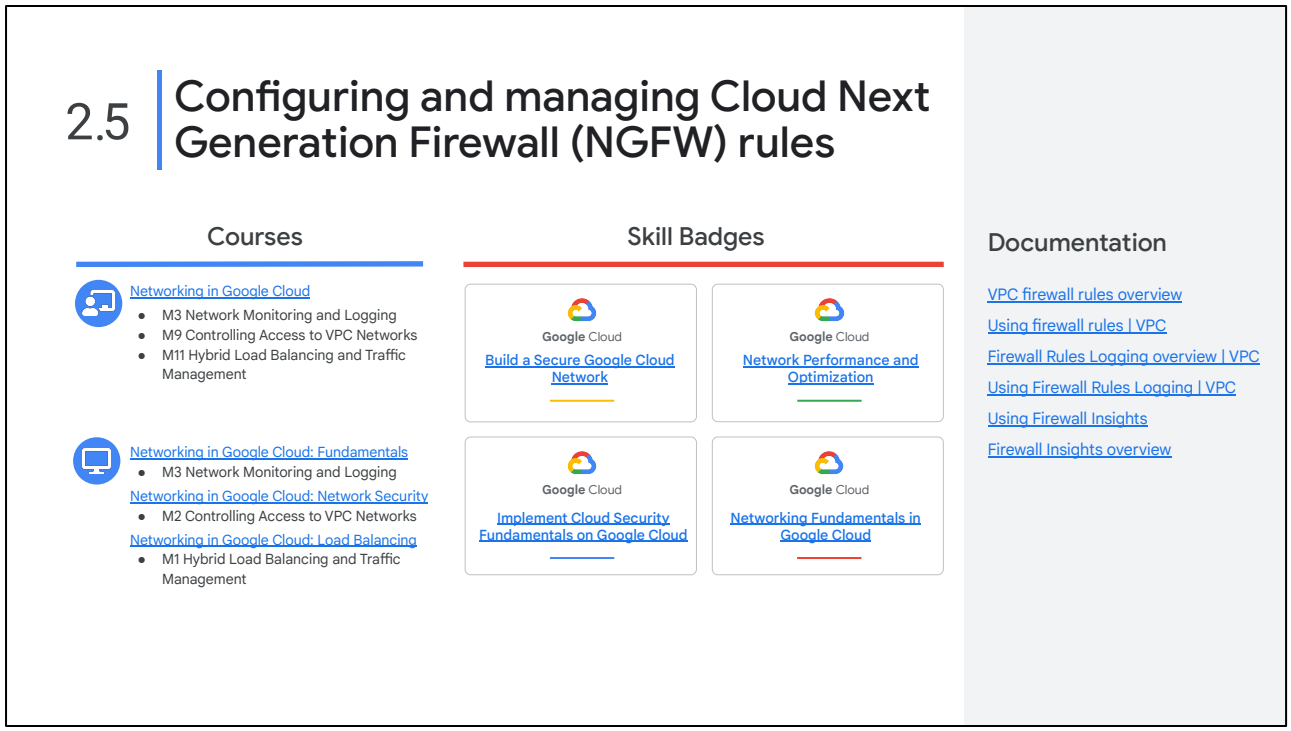
- ILT course: **Networking in Google Cloud**
  - M3 Network Monitoring and Logging

- On-demand course: **Networking in Google Cloud: Fundamentals**
    - M3 Network Monitoring and Logging

Summary:
Firewall Logging and Firewall Insights can be useful tools for troubleshooting firewall configuration problems. They must be enabled and properly configured before usage. Firewall Insights provides high-level details for quick analysis and detection of problems, such as shadowed rules, overly permissive rules, and active deny rules. It doesn't directly provide detailed information about the firewall rule activity.

Firewall Insights can be combined with filtering on matching firewall logs to get more of the details. Firewall logs capture all of the detailed information about firewall activity but can produce large logs. These logs may require filtering to effectively find activity related to the traffic flows of interest.

When troubleshooting, it's also important to remember that logs and insights are not captured for the implicit deny all ingress and allow all egress firewall rules.



Let's consider resources that can help you build your knowledge and skills in this area.

The concepts in the diagnostic questions we just reviewed are covered in these modules and in this documentation. You'll find this list in your workbook so you can take a note of what you want to include later when you build your study plan. Based on your experience with the diagnostic questions, you may want to include some or all of these.

Networking in Google Cloud (ILT)
Networking in Google Cloud: Fundamentals (On-demand)
Networking in Google Cloud: Network Security (On-demand)
Networking in Google Cloud: Load Balancing (On-demand)

Build a Secure Google Cloud Network (Skill badge)
Implement Cloud Security Fundamentals on Google Cloud (Skill badge)
Network Performance and Optimization (Skill badge)
Networking Fundamentals in Google Cloud (Skill badge)

https://cloud.google.com/vpc/docs/firewalls
https://cloud.google.com/vpc/docs/using-firewalls
https://cloud.google.com/vpc/docs/firewall-rules-logging
https://cloud.google.com/vpc/docs/using-firewall-rules-logging
https://cloud.google.com/network-intelligence-center/docs/firewall-insights/how-to/usin

g-firewall-insights
https://cloud.google.com/network-intelligence-center/docs/firewall-insights/concepts/overview