



Networking in Google Cloud

VPC Networking Fundamentals

Welcome to the first module VPC Networking Fundamentals.



Today's agenda



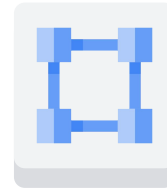
- 01 [VPC networks](#)
- 02 Multiple network interfaces
- 03 Lab: Working with Multiple VPC Networks
- 04 Network Service Tiers
- 05 Quiz

This module dives into the fundamentals of Virtual Private Cloud (VPC) networks, guiding you through managing multiple network interfaces efficiently. You'll also have the opportunity to apply your knowledge in hands-on labs. We will then explore Network Service Tiers and how it can be used to optimize performance. We will also cover a hand-on lab on optimizing network spend with network tiers and then wrap up the module with a final assessment.

At the end of the module, there will be a short quiz. Now, let's get started with the VPC networks.

A Virtual Private Cloud (VPC) network is a virtual version of a physical network that:

- ✓ Provides connectivity for your Compute Engine virtual machine (VM) instances.
- ✓ Offers built-in internal passthrough Network Load Balancers and proxy systems for internal Application Load Balancers.
- ✓ Distributes traffic from Google Cloud external load balancers to backends.



Virtual Private
Cloud Networks

A Virtual Private Cloud (VPC) network is a virtual version of a physical network that provides connectivity for your Compute Engine virtual machine (VM) instances, including Google Kubernetes Engine (GKE) clusters, App Engine flexible environment instances, and other Google Cloud products built on Compute Engine VMs.

Offers built-in internal passthrough Network Load Balancers and proxy systems for internal Application Load Balancers.

A VPC network connects to on-premises networks by using Cloud VPN tunnels and Cloud Interconnect attachments. It distributes traffic from Google Cloud external load balancers to backends.

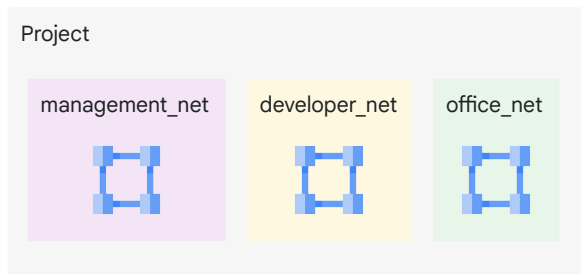
By default, every network has routes that let instances in a network send traffic directly to each other, even across subnets. In addition, every network has a default route that directs packets to destinations that are outside the network. Although these routes cover most of your normal routing needs, you can also create special routes that override these routes.

Just creating a route does not ensure that your packets will be received by the specified next hop. Firewall rules must also allow the packet.

The default network has pre-configured firewall rules that allow all instances in the network to talk with each other. Manually created networks do not have such rules, so you must create them.


VPC networks

- ✓ Projects can contain multiple VPC networks.
- ✓ New projects start with a default network (an auto mode VPC network) that has one subnetwork (subnet) in each region.
- Google-recommended practice: create a custom mode VPC network.




Projects can contain multiple VPC networks. Unless you create an organizational policy that prohibits it, new projects start with a default network (an auto mode VPC network) that has one subnetwork (subnet) in each region.

An auto mode VPC network can be useful when you start learning about Google Cloud. However, it's a best practice to create a custom mode network and include subnetworks only in desired regions.



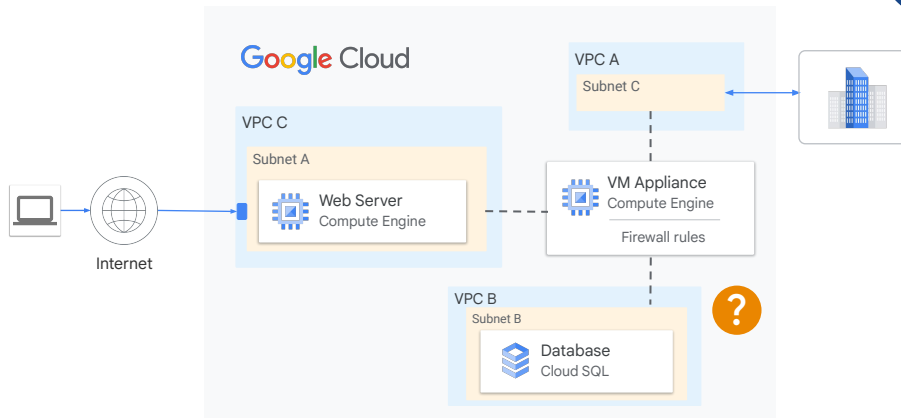
Today's agenda



- 01 VPC networks
- 02 [Multiple network interfaces](#)
- 03 Lab: Working with Multiple VPC Networks
- 04 Network Service Tiers
- 05 Quiz

In conventional networking, devices can use multiple network interfaces to communicate with multiple networks. Next, let's discuss using multiple network interfaces in a Google Cloud VPC network.

Use case: Interconnect multiple networks to a virtual appliance

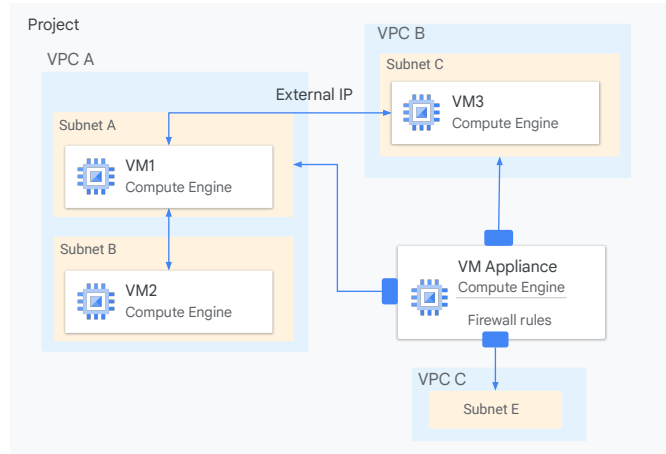


Sasha is a network engineer at Cymbal Corporation. Cymbal is rolling out a new web-based customer portal. This portal will give access to sensitive account data and the capability to initiate transactions. The environment also has a management network that connects to the on-premises environment using a VPN. For compliance and security purposes, Sasha is looking to filter control plane traffic from data plane traffic. She is thinking of using a security virtual appliance to route traffic between VPC networks, to an on-premises environment and to the internet. This means she needs a mechanism to interconnect multiple networks to a single virtual appliance.

Let us look into how we can solve this use case.

VPC networks are isolated by default

- ✓ VPC networks
 - Use an internal IP to communicate within networks.
 - Use an external IP to communicate across networks.
- ✓ Use multiple network interfaces when you need a single instance to act as a network appliance for tasks like load balancing, intrusion detection/prevention (IDS/IPS), and more.



VPC networks are isolated private networking domains by default. As we mentioned earlier, VM instances within a VPC network can communicate among themselves by using internal IP addresses as long as firewall rules allow it. However, no internal IP address communication is allowed between networks unless you set up mechanisms such as VPC peering or VPN.

Every VM instance within a VPC network starts with a built-in default network interface. When you add more interfaces, you must choose a VPC network and a subnet within it for each new interface. Importantly, each additional interface has to connect to a different VPC network than the others. This multi-interface setup lets you establish configurations where a single instance directly connects to multiple VPC networks. Use multiple network interfaces when you need a single instance to act as a network appliance for tasks like load balancing, intrusion detection/prevention (IDS/IPS), and web application firewalls (WAF).

In the diagram,

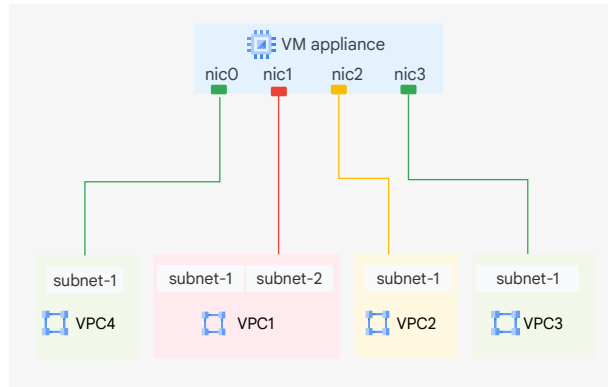
- VM1 communicates with VM2 through an internal IP address.
- VM1 communicates with VM3 through an external IP address
- VM appliance communicates with VM1 and VM3 through NIC.

Network interface controllers

Each NIC:

- ✓ Is attached to a separate VPC network.
- ✓ Uses an internal IP to communicate across networks.

You cannot add or remove NICs once an instance is created.



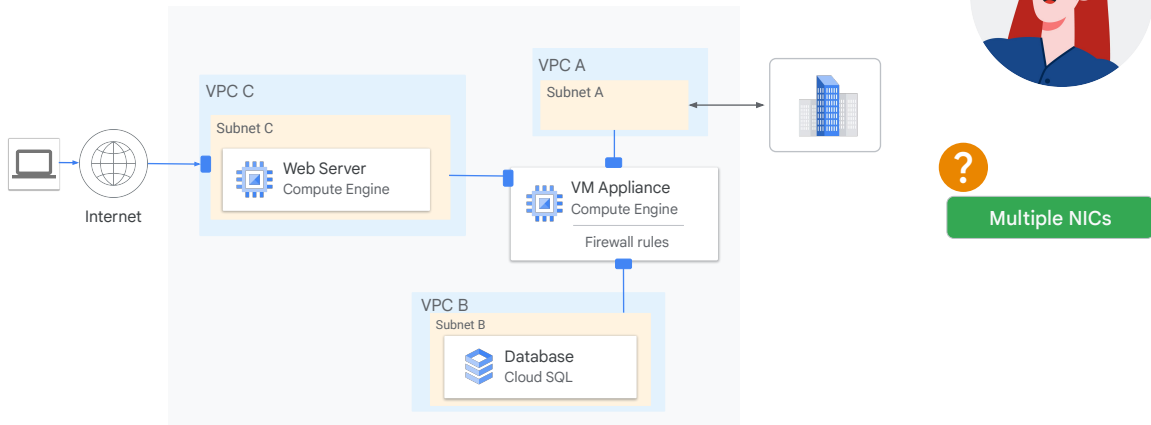
Multiple network interfaces let you create configurations in which an instance connects directly to several VPC networks. Each of the interfaces must have an internal IP address, and each interface can also have an external IP address.

For example, in this diagram, you have two VM instances. Each instance has network interfaces to a subnet within VPC1, VPC2, VPC3, and VPC4.

For some situations, you might require multiple interfaces. For example, to configure an instance as a network appliance for load balancing. Multiple network interfaces are also useful when applications running in an instance require traffic separation, such as separation of data plane traffic from management plane traffic.

Also, you cannot add or remove NICs to an instance once the instance is created. So, make sure to add the required NICs when you create the instance.

What Sasha can do



Going back to the use case.

The simplest way Sasha can connect multiple networks to a VM appliance is by using multiple network interfaces. The diagram shows multiple VPC networks connecting through a virtual appliance using multiple network interfaces. Each interface connects to one of the VPC networks. The diagram also shows internet and on-premises connections over separate network interfaces, including an internet connection through an untrusted interface.

By configuring multiple interfaces, you can apply separate firewall rules and access controls to each interface separately, and enforce security functions in communications from the public to a private domain.

Multiple network interface caveats

01

Network interfaces can only be configured when you create an instance.

02

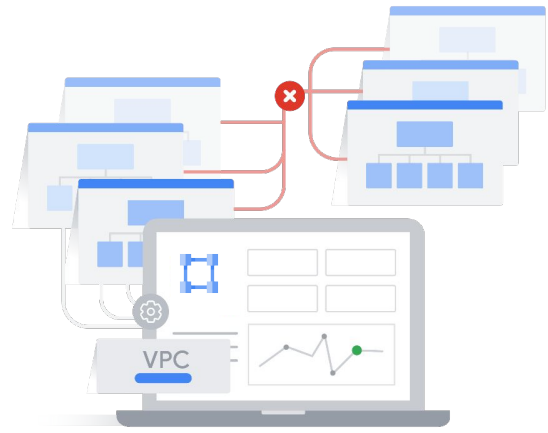
Each interface must be in a different network.

03

The network IP ranges cannot overlap.

04

The networks must exist before you create the VM.



When creating VM instances with multiple network interfaces, note these caveats.

You can only configure a network interface when you create an instance.

Each network interface configured in a single instance must be attached to a different VPC network. Each interface must belong to a subnet whose IP range does not overlap with the subnets of any other interfaces.

The additional VPC networks that the multiple interfaces will attach to must exist before you create the instance.

Multiple network interface caveats

- ✓ You cannot delete an interface without deleting the VM.
- ✓ The internal DNS (Domain Name System) is only associated to `nic0`.
- ✓ You can have up to 8 NICs, depending on the VM.

Type of instance	Total # of virtual NICs
VM <= 2 vCPU	2 NICs
VM >2vCPU	1 NIC per vCPU (Max: 8)


You cannot delete a network interface without deleting the instance.

When an internal DNS (Domain Name System) query is made with the instance hostname, it resolves to the primary interface (`nic0`) of the instance. If the `nic0` interface of the instance belongs to a different VPC network than the instance that issues the internal DNS query, the query will fail. You will explore this in the upcoming lab.


The maximum number of network interfaces per instance is 8, but this depends on the instance's machine type, as shown in this table:

Instances with less than or equal to 2 vCPU can have up to 2 virtual NICs. Examples include the `f1-micro`, `g1-small`, `n1-standard-1`, and any other custom VMs with 1 or 2 vCPUs.

Instances with more than 2 vCPU can have 1 NIC per vCPU, with a maximum of 8 virtual NICs.



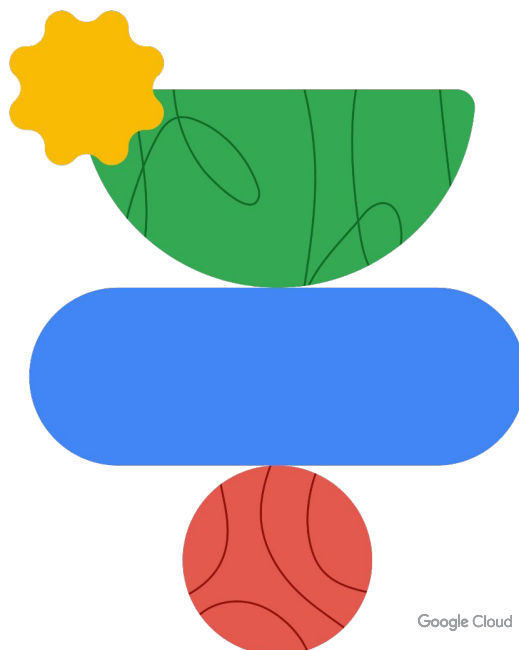
Today's agenda



- 01 VPC networks
- 02 Multiple network interfaces
- 03 [Lab: Working with Multiple VPC Networks](#)
- 04 Network Service Tiers
- 05 Quiz

Lab intro


Working with Multiple VPC
Networks




Google Cloud

In this lab, you create several VPC networks and VM instances and test connectivity across networks. The lab tasks are to:

- Create custom mode VPC networks with firewall rules.
- Create VM instances by using Compute Engine.
- Explore the connectivity for VM instances across VPC networks.
- Create a VM instance with multiple network interfaces.



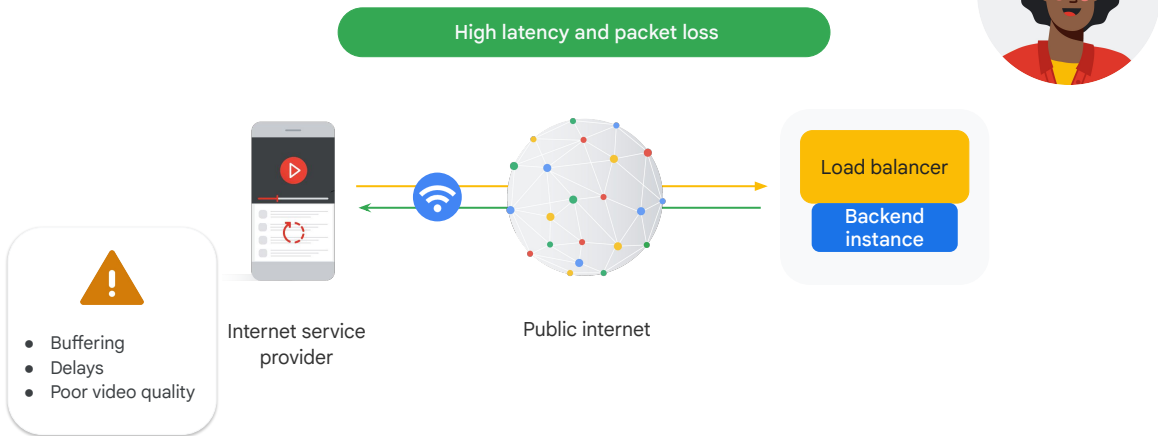
Today's agenda



- 01 VPC networks
- 02 Multiple network interfaces
- 03 Lab: Working with Multiple VPC Networks
- 04 [Network Service Tiers](#)
- 05 Quiz

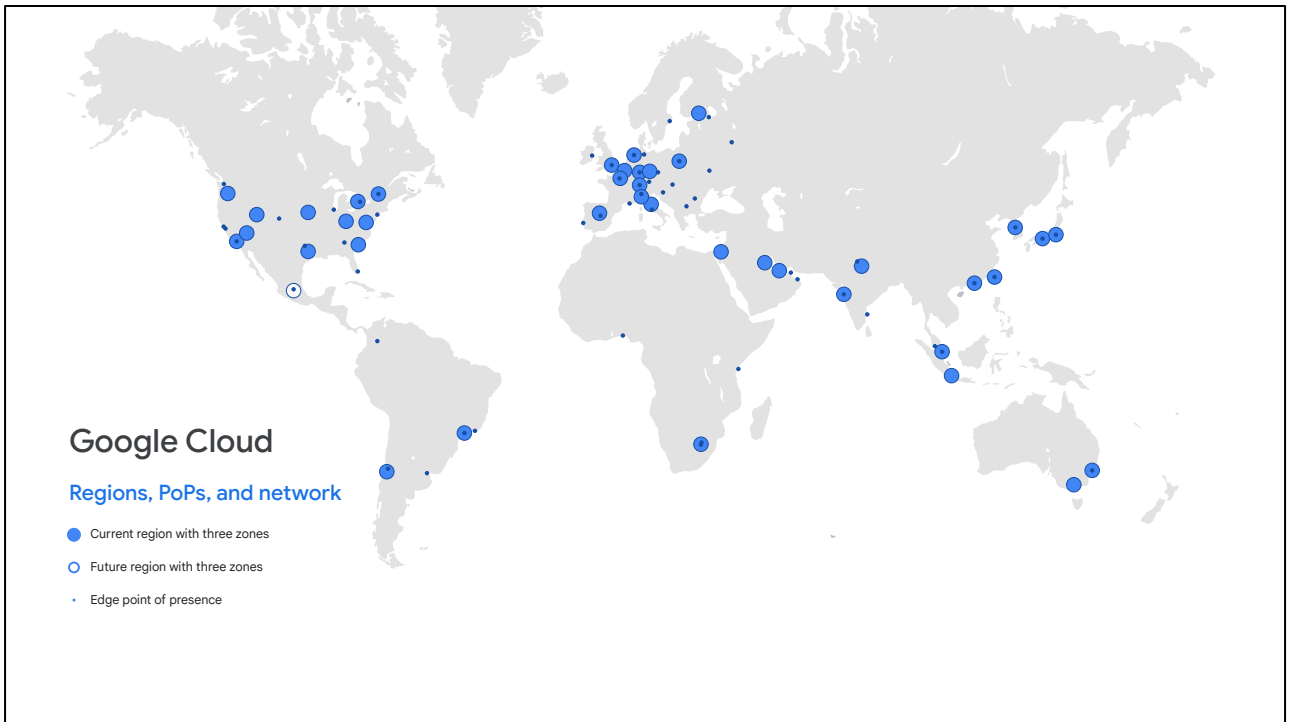
Next, let's talk about how Network Service Tiers helps boost your network performance.

Improve network performance



To illustrate this, consider the following scenario. Sarah, a network engineer at Cymbal Corporation, is facing a challenge. Their video streaming platform is experiencing high latency and inconsistent performance, especially during peak hours. The current network infrastructure struggles to keep up with the growing number of global users. The user request traverses the internet. Finally, the request arrives at the load balancer in Google Cloud. Google Cloud cannot control the user experience on the internet, so the provider has no way to deliver low latency and great user experience.

What can Sarah do to reduce latency and optimize performance?



Premium Tier delivers traffic on Google's premium backbone, while Standard Tier uses regular ISP networks.

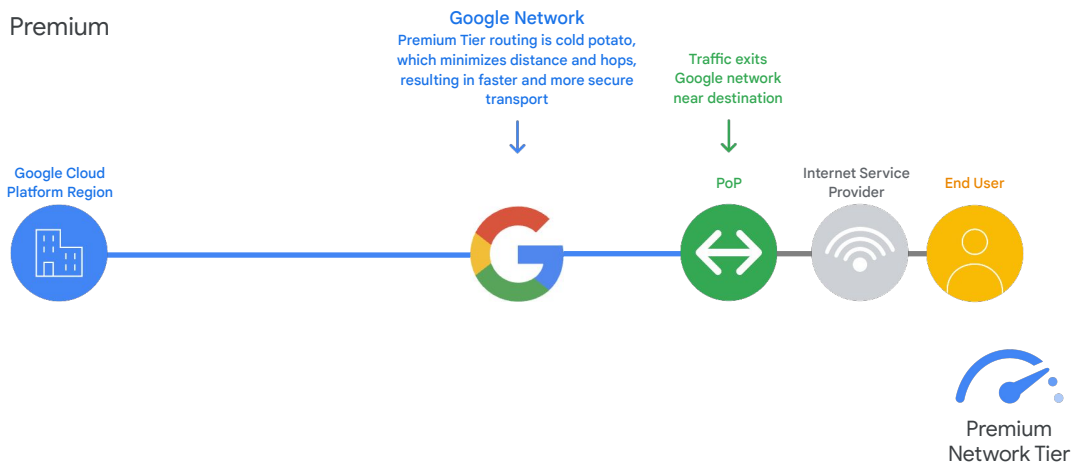
As you can see on this map, this network consists of an extensive global private fiber network with over 100 points of presence across the globe.

Let's explore each Network Service Tier to better understand network performance and cost differences. This information is subject to change. For more accurate and current details, please use this [link](https://cloud.google.com/about/locations#network) [<https://cloud.google.com/about/locations#network>].

See www.gcping.com for information on latency displayed by region.

Optimize performance with Premium Tier

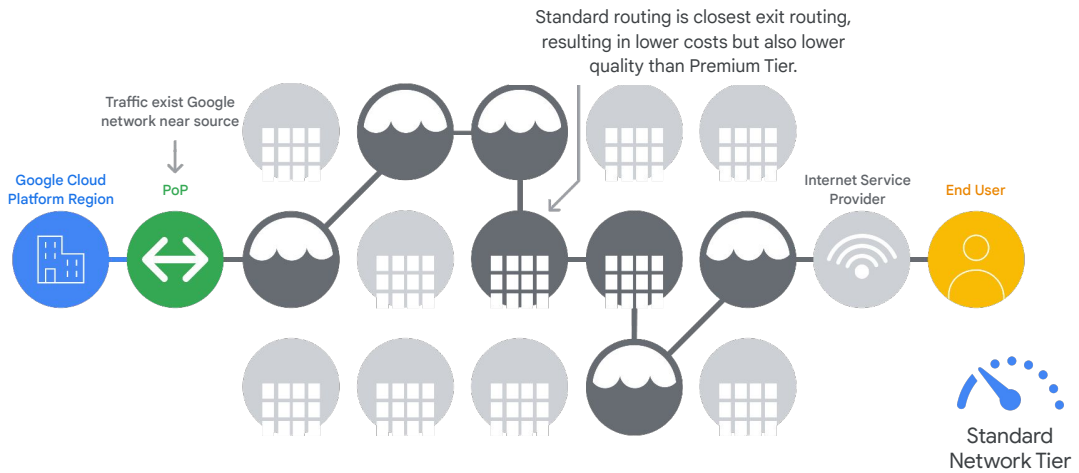
Premium



In Premium Tier, inbound traffic from the end user to the video streaming application in Google Cloud enters Google's private, high-performance network at the POP closest to your end user, and Google Cloud delivers this traffic to your application over this network.

Similarly, Google Cloud delivers outbound traffic from the application to end users on Google's network and exits at the POP closest to them, wherever the end users are across the globe. This means that most of this traffic will reach its destination with a single hop to the end user's ISP, so it enjoys minimum congestion and maximum performance.

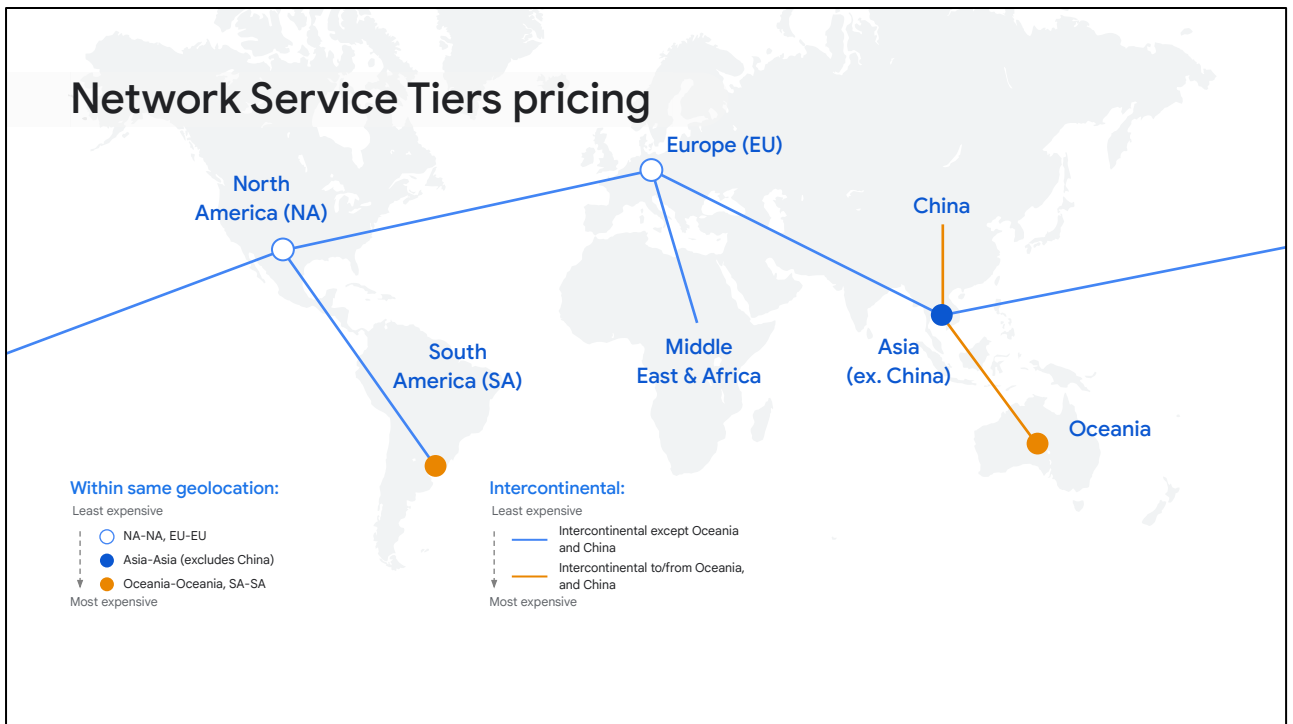
Optimize cost with Standard Tier



Sarah could also use Standard Tier. Standard Tier provides network quality that is comparable to other public cloud providers, but lower than Premium Tier. Also, regional network services such as regional load balancing have one VIP per region.

Standard tier is priced lower than Premium because your traffic between Google Cloud and your end user is delivered over ISP networks instead of Google's network.

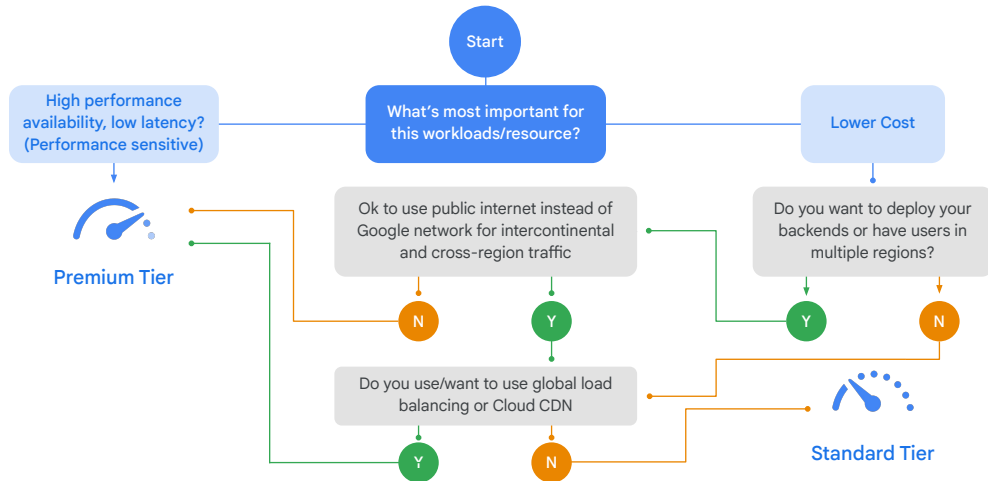
Now that you understand the differences in performance, let's get into cost.



Premium Tier pricing is based on both source and destination of traffic. This is because the cost of network traffic varies depending on the distance your traffic travels over Google's network. In contrast, Standard Tier traffic is source-based because it does not travel much over Google's network.

This map illustrates that Network Service Tiers categorizes all countries and continents into the listed geolocations. Depending on the origin and destination of traffic, costs will vary.

Network Service Tiers decision tree



We have gone over both the performance and cost differences between Network Service Tiers. The decision tree will help Sarah decide on the tier that best meets the organization needs.

For your specific workload or resource, what holds higher priority? Exceptional performance or cost optimization? The Premium Tier is the clear choice for performance. If cost is the main consideration, remember that the Standard Tier has other restrictions in addition to network performance. If you want to deploy your backends, have users in multiple regions, but don't want to use the public internet instead of Google's network for intercontinental and cross-region traffic, you want to choose the Premium Tier.

Also, if you want global load balancing or Cloud CDN, you need to use the Premium Tier.

The Standard Tier is a great choice if you don't need any of those services and are okay using the public internet instead of Google's network.

Use Network Service Tiers to optimize your network for performance or cost

Premium Tier	Standard Tier
High performance routing (Google's network)	Lower price and performance than Premium Tier
Unique to Google Cloud	Comparable to other public cloud offerings
99.99% uptime	99.9% uptime
Regional and global external IPv4 and IPV6 addresses	Regional external IPv4 addresses (not BYOIP)
External global and regional load balancer, VM instances including GKE nodes, Cloud NAT and Cloud VPN	Foundational feature set including Cloud NAT, Regional external Application Load Balancer, and External passthrough Network Load Balancer
Performance is main consideration	Cost is main consideration

Network Service Tiers enable Sarah to optimize your cloud network for performance by choosing Premium Tier or for cost with the new Standard Tier. So what is the difference between these two tiers?

The Premium Tier delivers traffic on Google's global network, providing high-performance routing. If Sarah uses Google Cloud today, Sarah already uses the powerful Premium Tier. The Standard Tier, alternatively, offers an attractively priced network with a performance comparable to that of other major public clouds.

There are other differences between the two tiers. The SLA is 99.99% for Premium and 99.9% for Standard Tier. Premium Tier also supports regional and global external IPv4 addresses and Standard Tier supports regional external IPv4 addresses. Premium also allows for all Google Cloud networking features and the Standard Tier provides a wide variety of foundational feature set such as Cloud NAT, external Application Load Balancer, and External passthrough Network Load Balancer.

So why would Sarah choose the Standard Tier? Well, it all comes back to optimizing the cloud network for performance by choosing Premium Tier or for cost with the Standard Tier. In other words, Network Service Tiers allows Sarah to design the cloud network her way.

Let's explore each feature in Network Service Tiers to better understand network performance and cost differences. Refer to the documentation for a detailed list and more information at <https://cloud.google.com/network-tiers/docs/overview>.

Let's ask Gemini



How can I use gcloud to create my first VPC network in Google Cloud?



To create a VPC network using the gcloud CLI, follow these steps:

1. In the Google Cloud console, activate Cloud Shell.
2. Run the following command:

```
gcloud compute networks create NETWORK_NAME --subnet-mode=CUSTOM
```

Replace NETWORK_NAME with the name of your network

To create a subnet in your new VPC network, run the following command:

```
gcloud compute networks subnets create SUBNET_NAME \  
  --network=NETWORK_NAME \  
  --range=SUBNET_RANGE \  
  --region=REGION
```

*Gemini responses may vary


Google Cloud

If you still are not sure where to start and how, you can always lean on Gemini, an AI-powered collaborator in Google Cloud, for some help. Wondering how?


Ensure that Gemini is set up for your Google Cloud user account and project and then you are all set to simply chat with Gemini to get help. Using the Gemini pane, you enter prompts, which are questions or statements that describe the help you want, and Gemini returns responses.

In the Google Cloud console toolbar, click chat_spark Open Gemini and type: How can I use gcloud to create my first VPC network in Google Cloud?

The response will cover instructions to create a simple VPC and a subnet. You can adjust to ask advanced steps by refining the prompt. For example, try, how can I adjust the gcloud command provided to create a subnet to ensure the subnet is dual-stack?



Today's agenda



- 01 VPC networks

- 02 Multiple network interfaces

- 03 Lab: Working with Multiple VPC Networks

- 04 Network Service Tiers

- 05 [Quiz](#)

Quiz | Question 1

Question

You are designing a virtual machine in the cloud to act as a network gateway between an external public network and a private internal network. To ensure strong security and traffic separation, what technology can you implement?

- A. Cloud VPN
- B. VLAN tagging within a single NIC
- C. Multiple Network Interface Cards (NICs)
- D. Premium Tier IPs

Explanation:

- A. While Cloud VPN is useful for external connections, it doesn't directly address internal segmentation.
- B. VLANs can help on a single NIC, but isolation might not be as strong as separate NICs.
- C. Load balancing is about distribution, not network separation.
- D. Multiple NICs attached to separate VPC networks achieve the strongest traffic isolation and control for the gateway scenario.

Quiz | Question 2

Question

You want to lower cloud networking cost and have no problem leveraging the public internet for cross-region traffic. Which network service tier is best for you?

- A. Premium Tier
- B. Standard Tier
- C. Pro version
- D. Prime tier

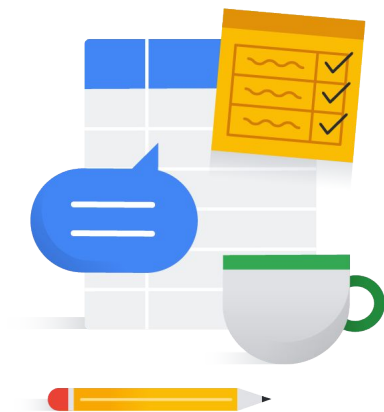
Quiz | Question 3

Question

You want to improve network performance. You are not comfortable using the public internet to route traffic. Which service tier is the best fit?

- A. Premium Tier
- B. Standard Tier
- C. Pro version
- D. Prime tier

Debrief



In this module, you learned about some fundamental Google Cloud VPC networking concepts. We began with an overview of Google Cloud VPC networks. Then, we discussed using multiple network interfaces on Compute Engine VMs, as well as some important caveats. After that, we discussed Network Service Tiers options and a use case. We concluded the module with a lab exercise and a brief quiz to test your knowledge of what you've learned.



THANK YOU