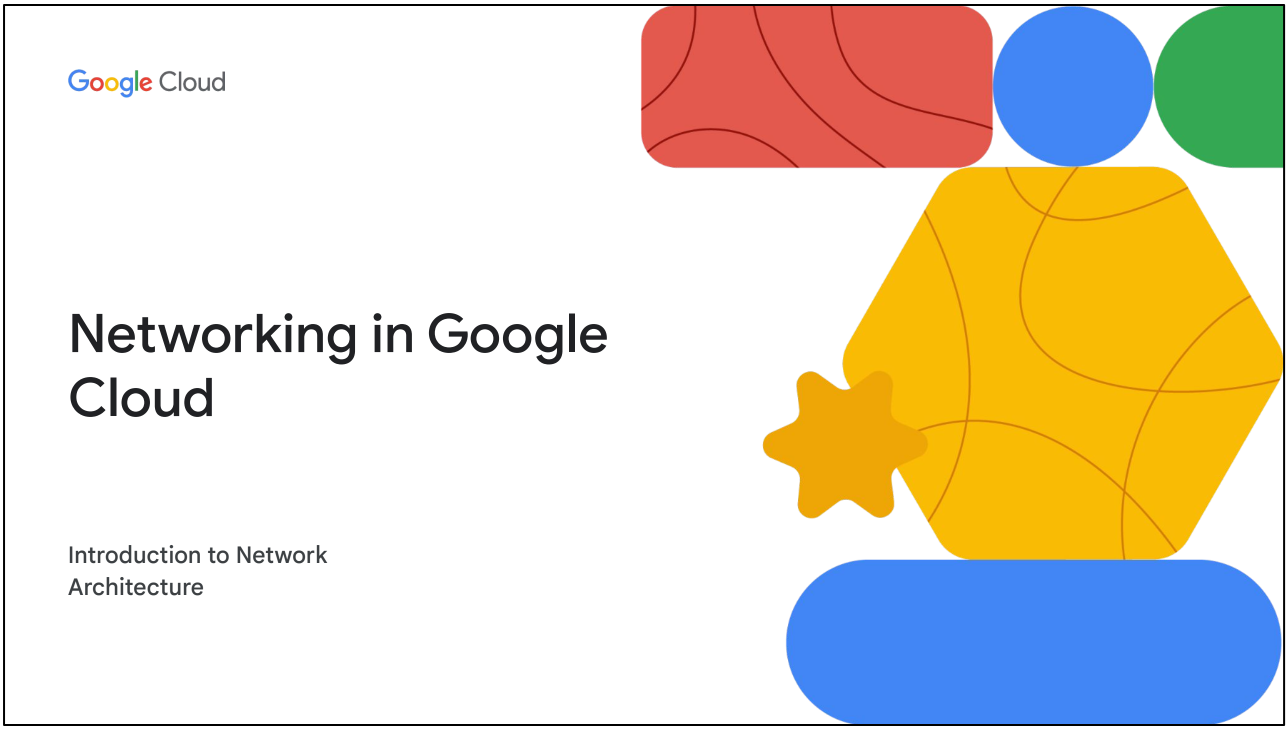
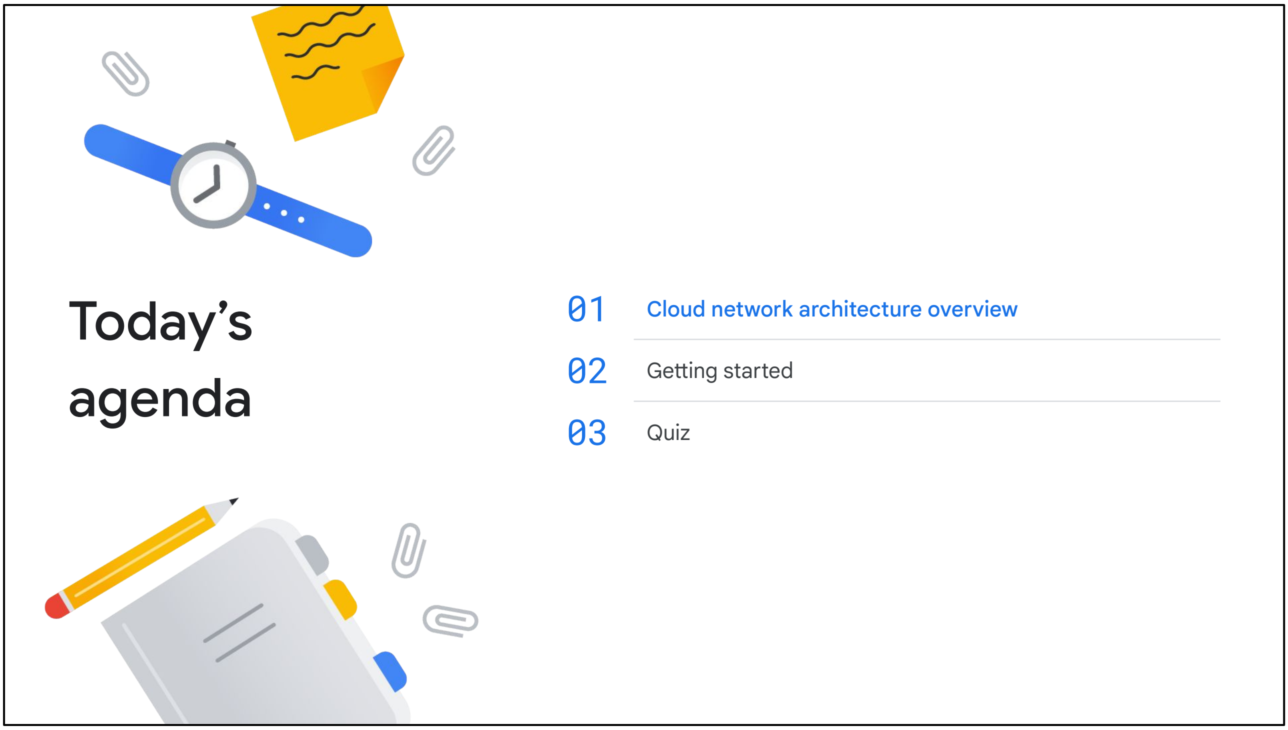


Google Cloud

Networking in Google Cloud

Introduction to Network Architecture

Welcome to the Introduction to Network Architecture module.



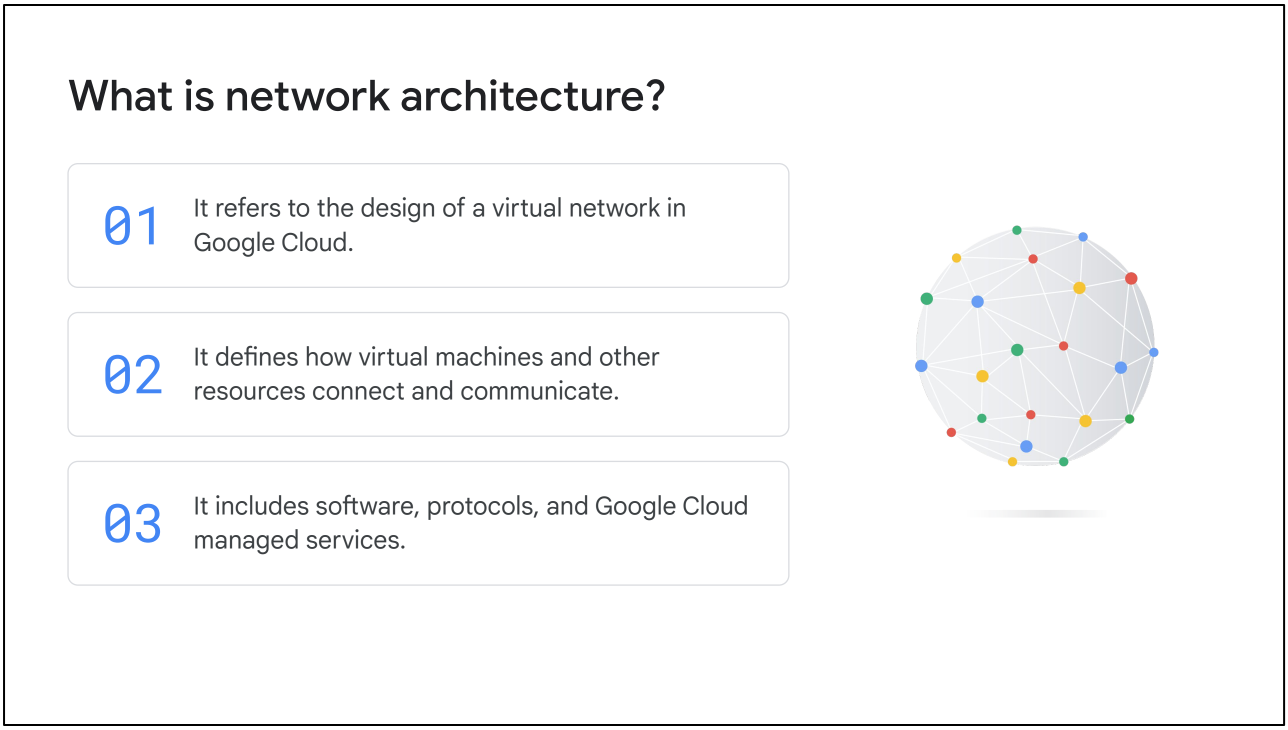
Today's agenda

01 Cloud network architecture overview

02 Getting started

03 Quiz

In this module, you are introduced to cloud network architecture. You will learn why good cloud network architecture is important and key points to consider when designing a network architecture for your environment. Let's begin with a cloud network architecture overview.



What is network architecture?

01 It refers to the design of a virtual network in Google Cloud.

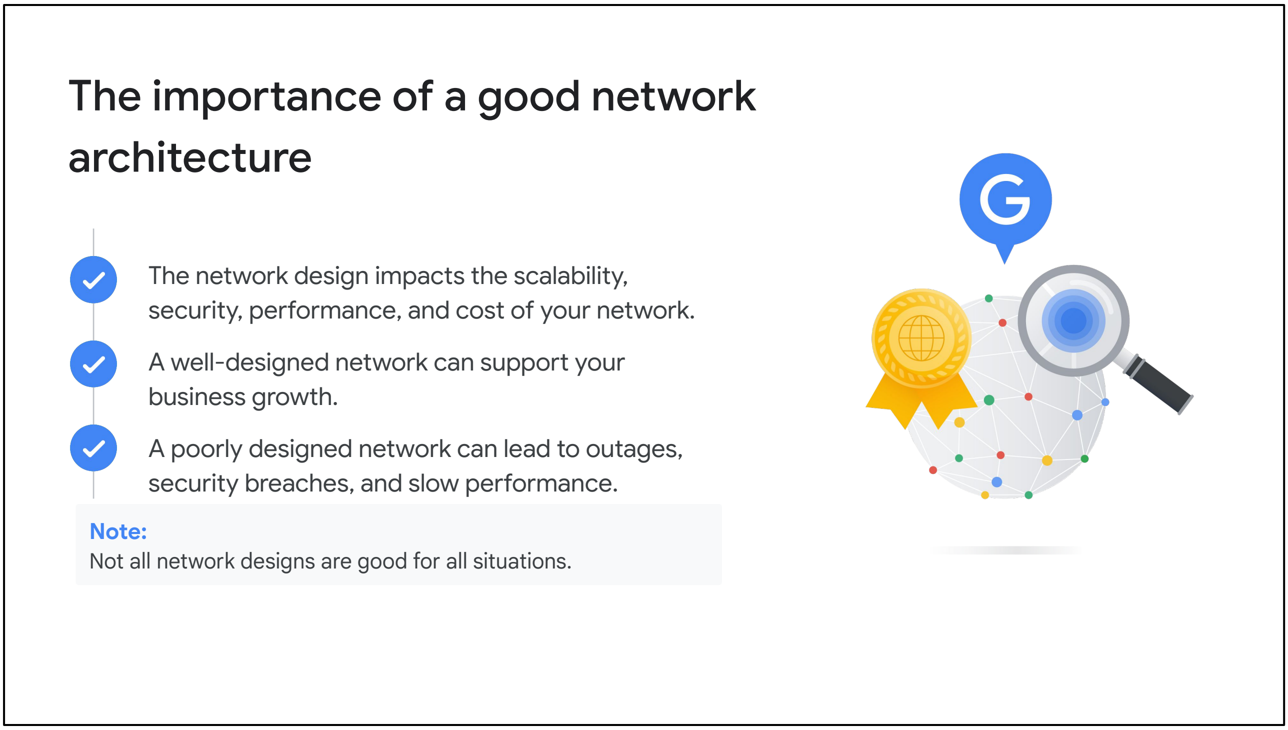
02 It defines how virtual machines and other resources connect and communicate.

03 It includes software, protocols, and Google Cloud managed services.

Network architecture refers to the design of a virtual network in Google Cloud.

It defines how virtual machines, containers, and other resources connect and communicate with each other within your cloud environment.

While Google manages the underlying physical infrastructure, you are responsible for configuring the software, protocols, and Google Cloud managed services that make up your virtual network. This includes components like VPC networks, subnets, firewalls, Cloud Routers, Cloud VPNs, and access points for on-premises connections.

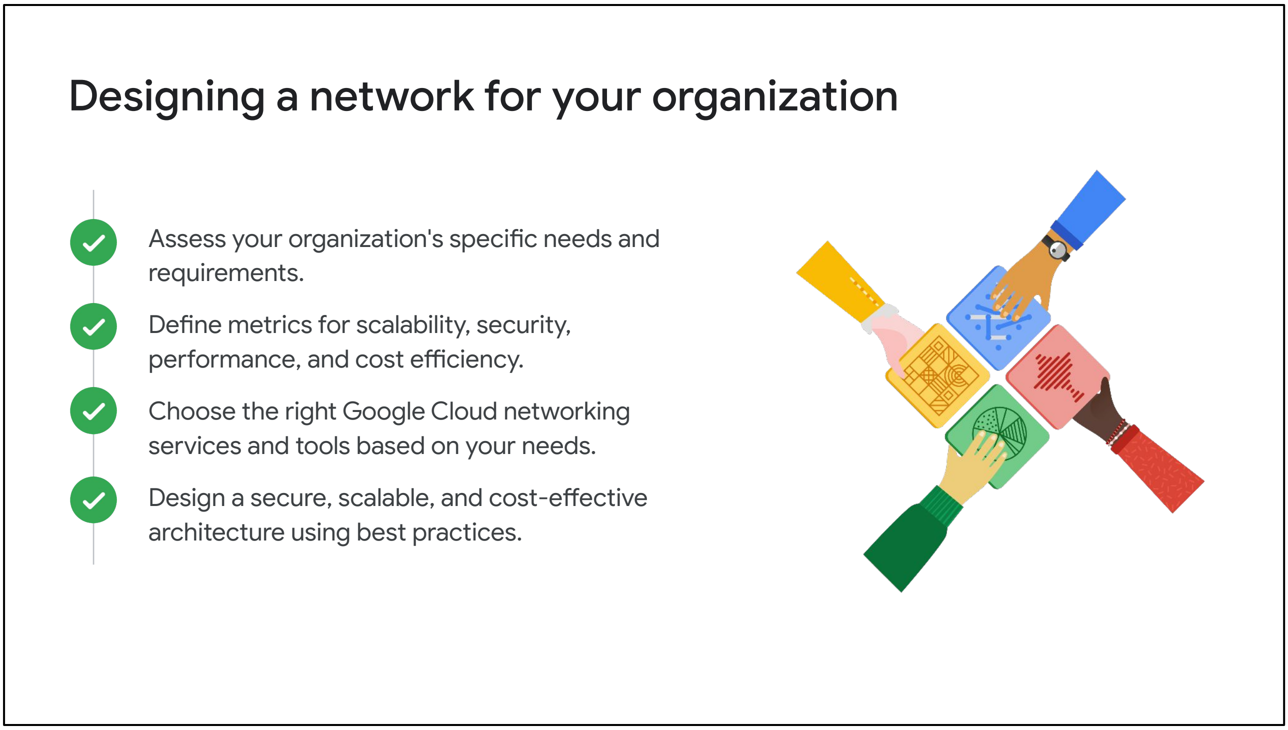


The importance of a good network architecture

- ✓ The network design impacts the scalability, security, performance, and cost of your network.
- ✓ A well-designed network can support your business growth.
- ✓ A poorly designed network can lead to outages, security breaches, and slow performance.

Note:
Not all network designs are good for all situations.

The network design impacts the scalability, security, performance, and cost of your network.
A well-designed network can support your business growth by providing the scalability, security, performance, and cost-efficiency you need.
On the other hand, a poorly designed network can lead to a number of problems, such as outages, security breaches, and slow performance. These problems can disrupt your business operations and damage your reputation.
Not all network designs are suitable for all situations. You select network components and protocols based on your organization’s needs and priorities.



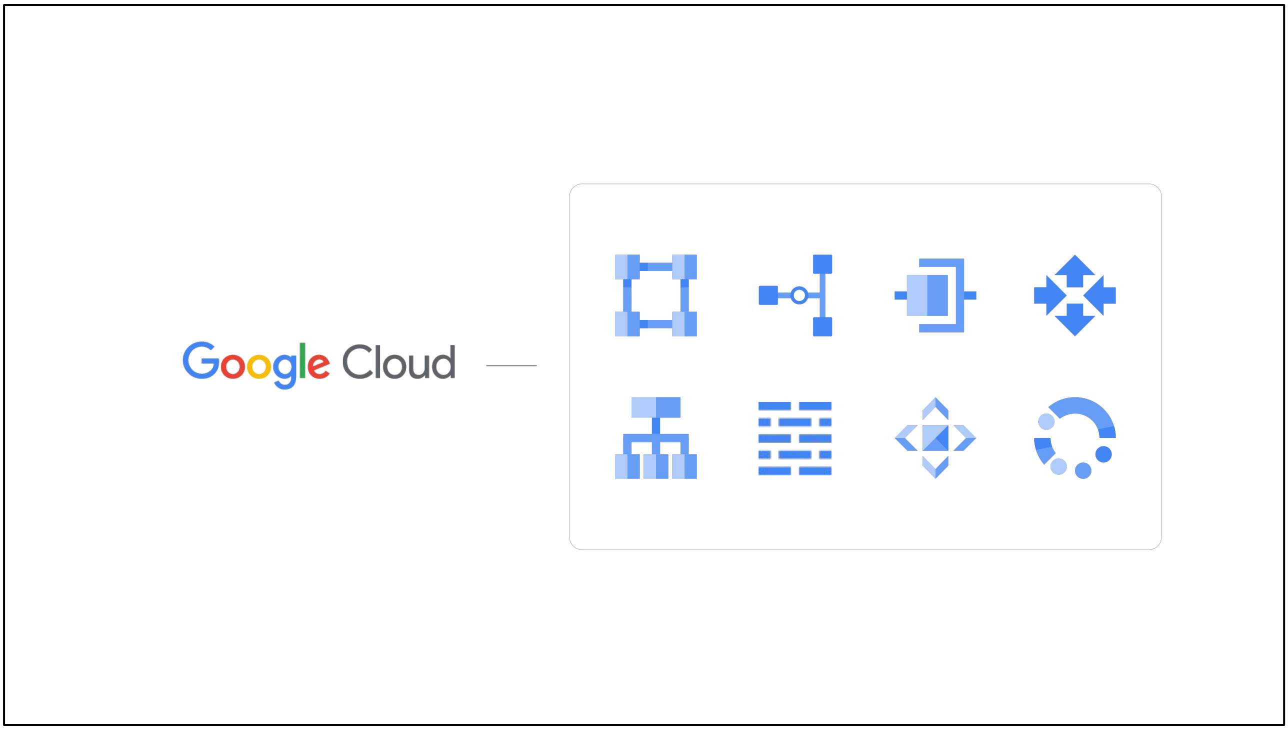
Designing a network for your organization

- ✓ Assess your organization's specific needs and requirements.
- ✓ Define metrics for scalability, security, performance, and cost efficiency.
- ✓ Choose the right Google Cloud networking services and tools based on your needs.
- ✓ Design a secure, scalable, and cost-effective architecture using best practices.

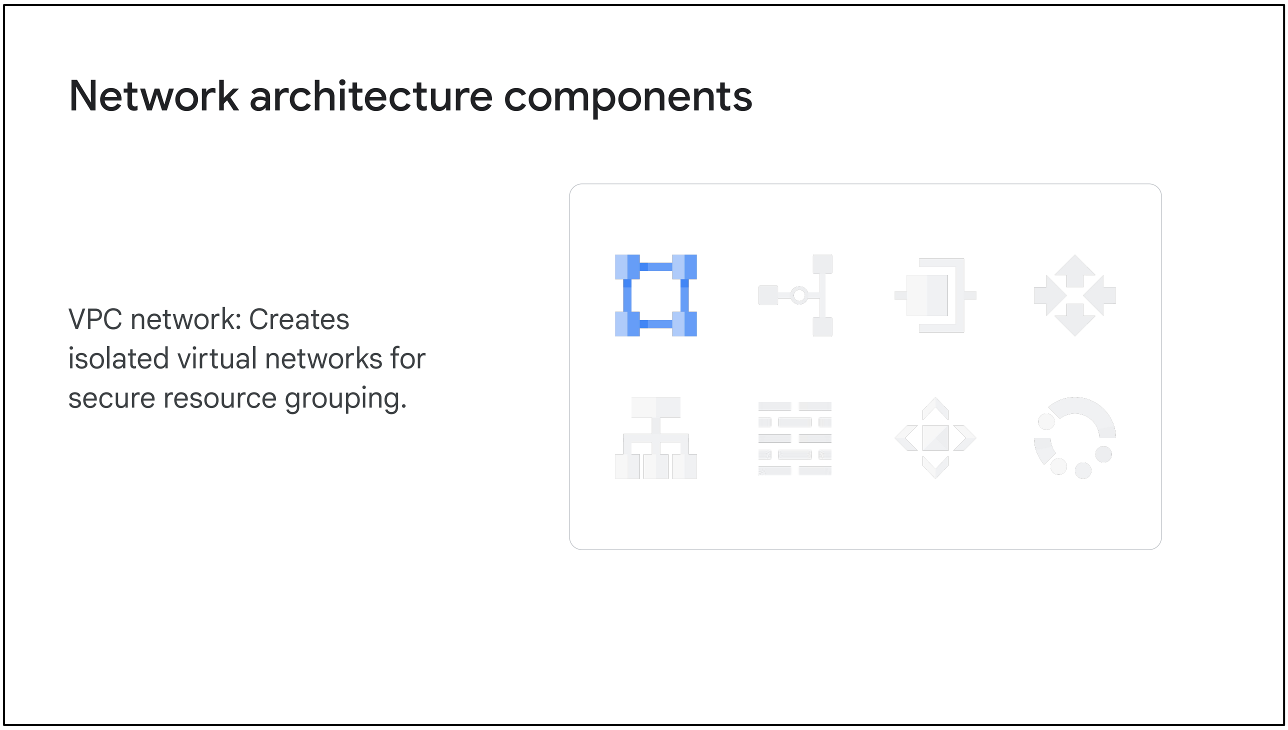
Tailoring your network architecture to your organization's specific needs is paramount. Start by thoroughly assessing your current and future requirements, considering factors like the number of users, applications, traffic volume, and security considerations.

Once you have a clear understanding of your needs, define quantifiable metrics for scalability, security, performance, and cost efficiency. These metrics can serve as a benchmark for evaluating your design choices. Google Cloud offers a comprehensive suite of networking services and tools.

Google Cloud offers a comprehensive suite of networking services and tools. Identify the ones that best suit your requirements and leverage them to craft a secure, scalable, and cost-effective network architecture.



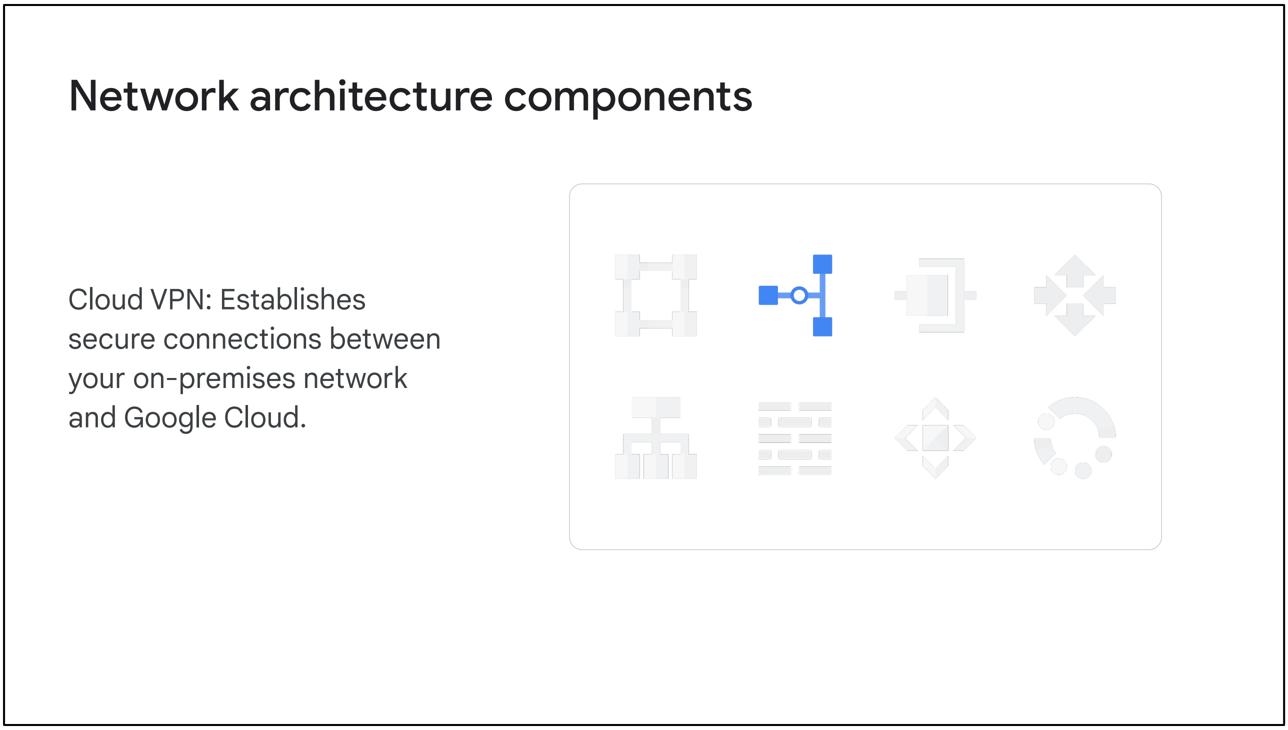
Google Cloud provides a powerful arsenal of networking services that enable you to build robust and optimized VPC networks. Each service plays a crucial role in achieving essential network characteristics like scalability, security, performance, and cost-efficiency.



Network architecture components

VPC network: Creates isolated virtual networks for secure resource grouping.

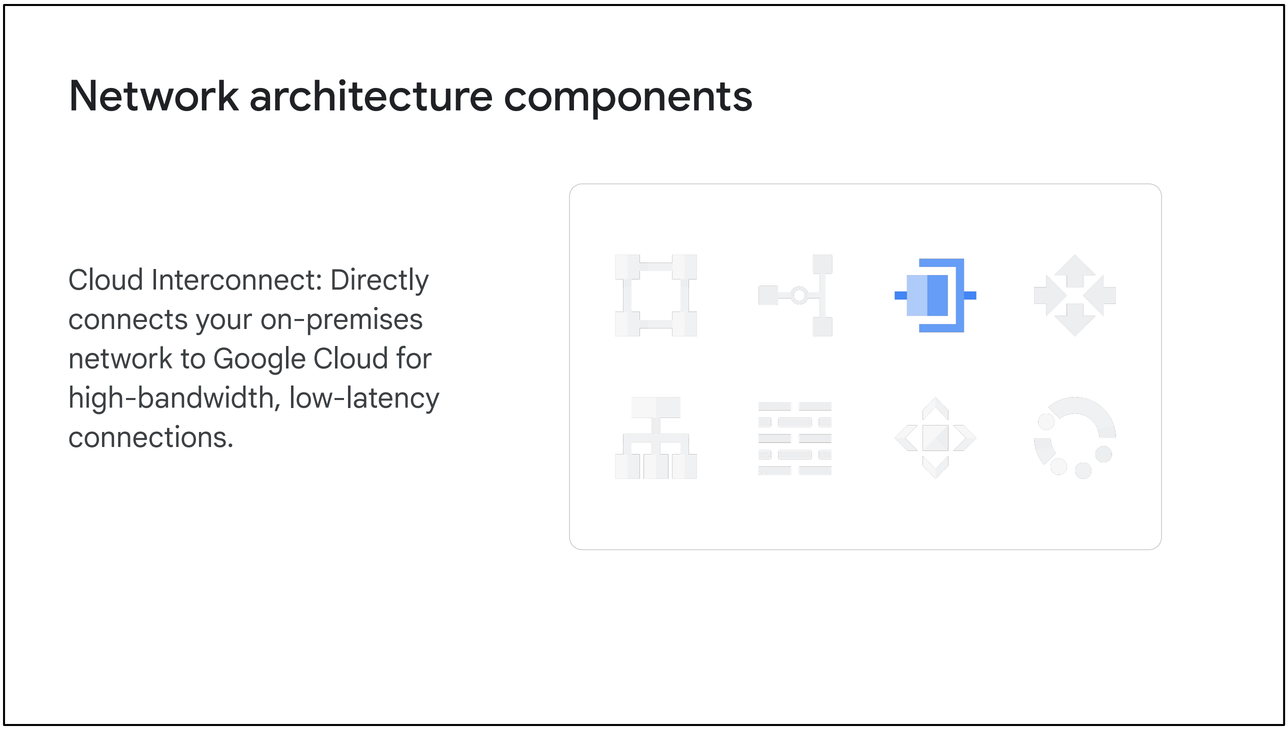
A VPC network enables secure resource grouping by segmenting your network into distinct subnets based on functionality, security considerations, or project boundaries. You have granular control over access lists and security policies within each VPC network.



Network architecture components

Cloud VPN: Establishes secure connections between your on-premises network and Google Cloud.

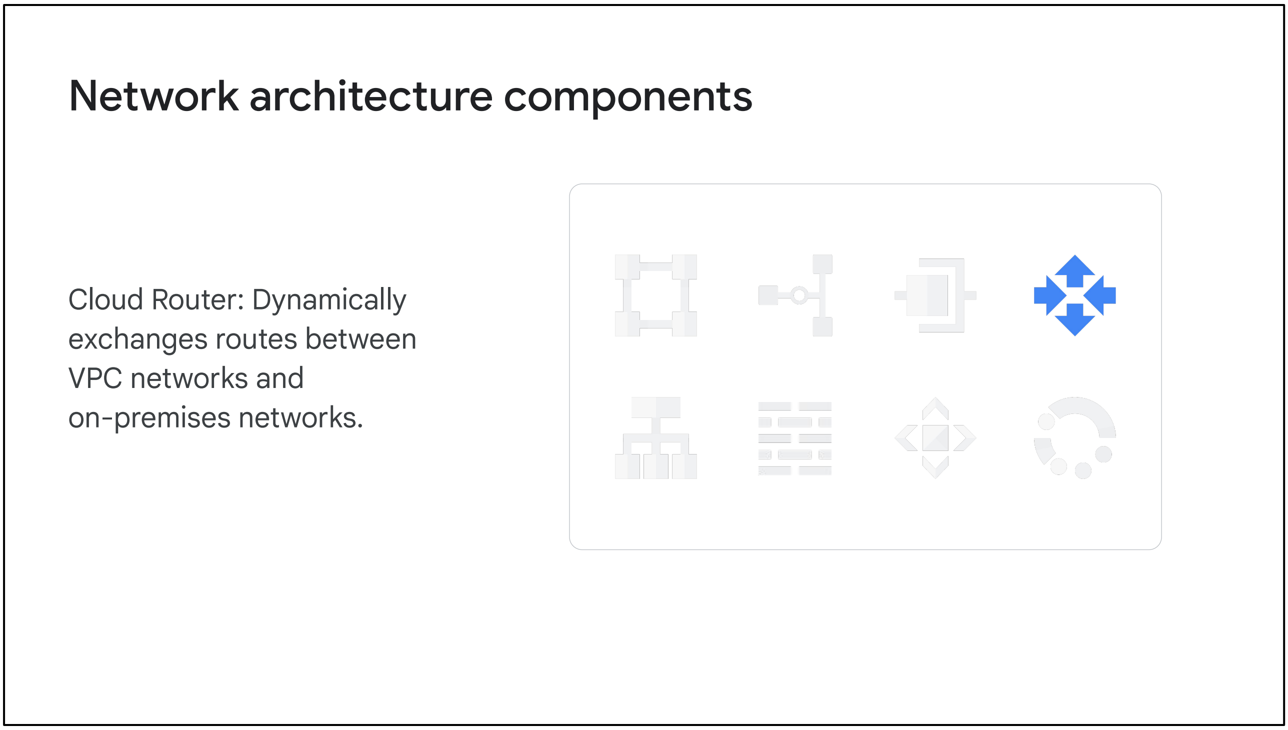
Cloud VPN establishes secure tunnels for encrypted data communication between your on-premises network and Google Cloud.



Network architecture components

Cloud Interconnect: Directly connects your on-premises network to Google Cloud for high-bandwidth, low-latency connections.

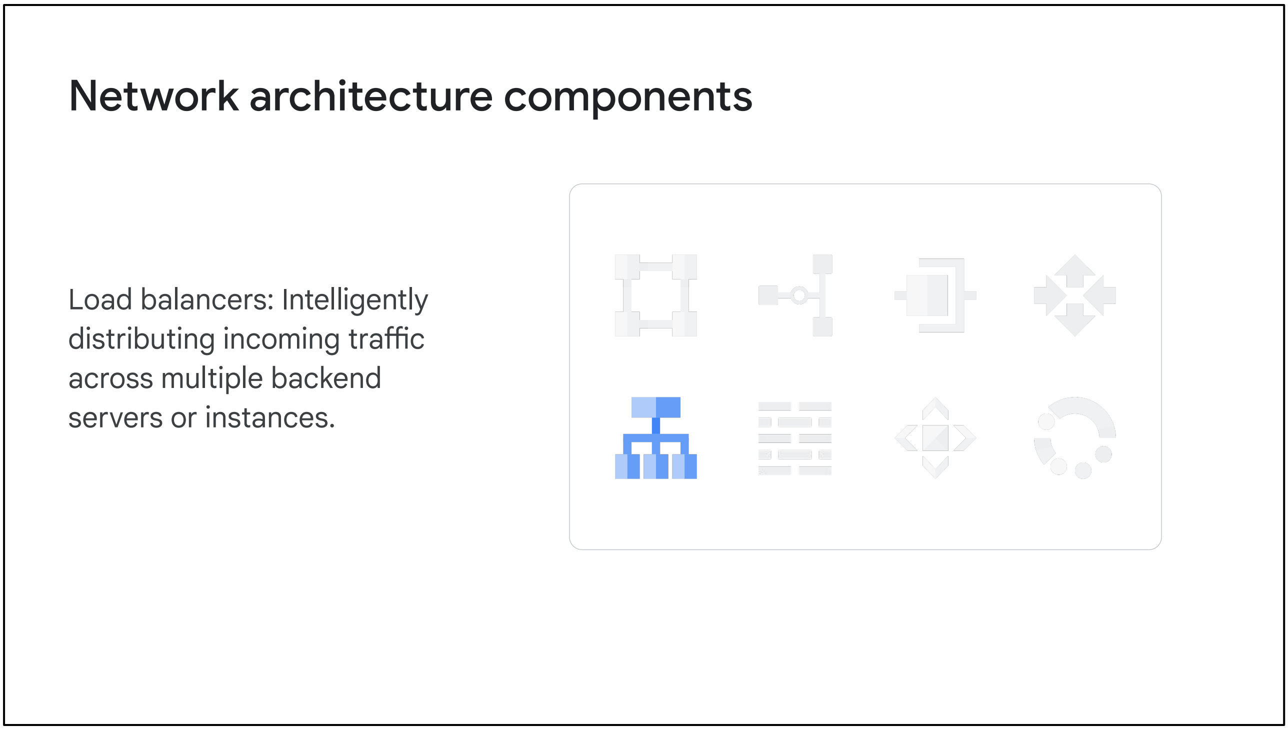
Cloud Interconnect directly provides high-bandwidth, low-latency connections between your on-premises network and Google Cloud. If needed, you can deploy Cloud VPN over Cloud Interconnect to provide encrypted data communication.



Network architecture components

Cloud Router: Dynamically exchanges routes between VPC networks and on-premises networks.

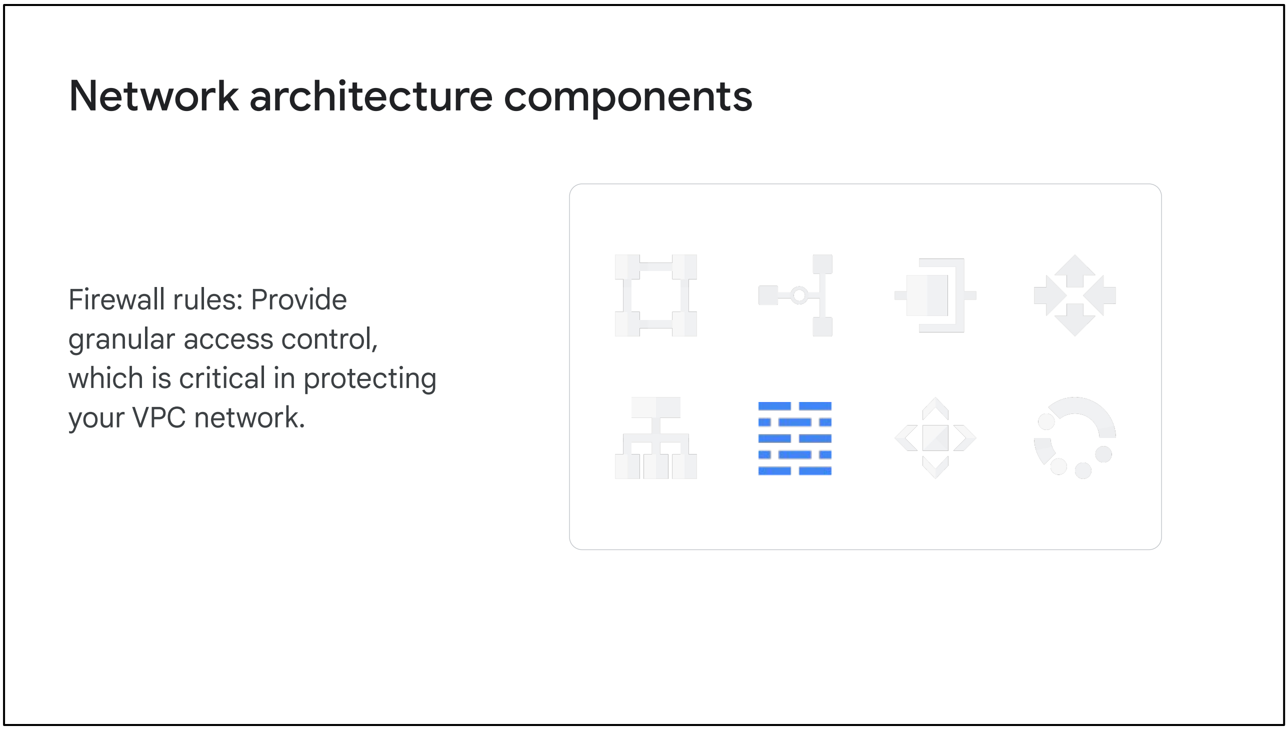
Cloud Router dynamically exchanges routes between Virtual Private Cloud Networks and on-premises networks. A Cloud Router also serves as the control plane for Cloud NAT. You have multiple configuration options, including policy-based routing and BGP peering. Cloud Router provides BGP services for the following Google Cloud products: Cloud Interconnect, Cloud VPN, and Router appliance.



Network architecture components

Load balancers: Intelligently distributing incoming traffic across multiple backend servers or instances.

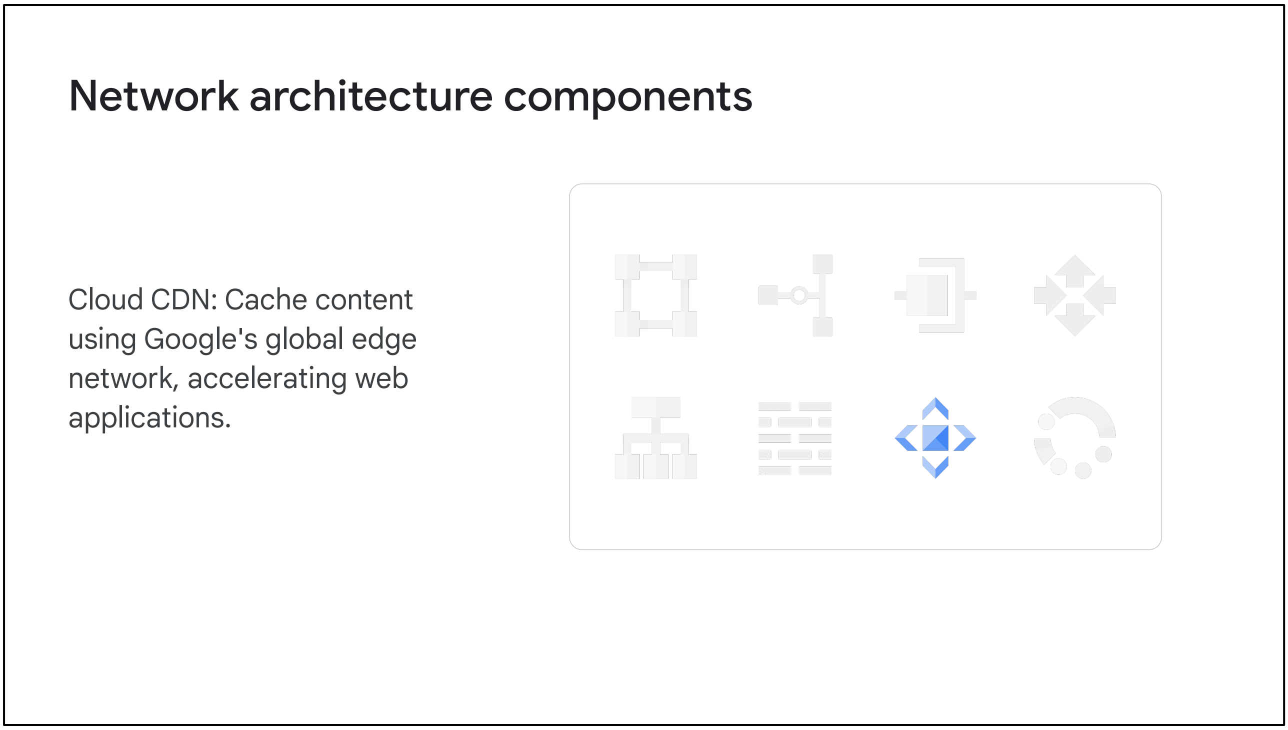
Load balancers play a vital role in cloud networks by intelligently distributing incoming traffic across multiple backend servers or instances. This optimization prevents overload on individual servers, enhancing performance, scalability, and ensuring high availability for your cloud-based applications.



Network architecture components

Firewall rules: Provide granular access control, which is critical in protecting your VPC network.

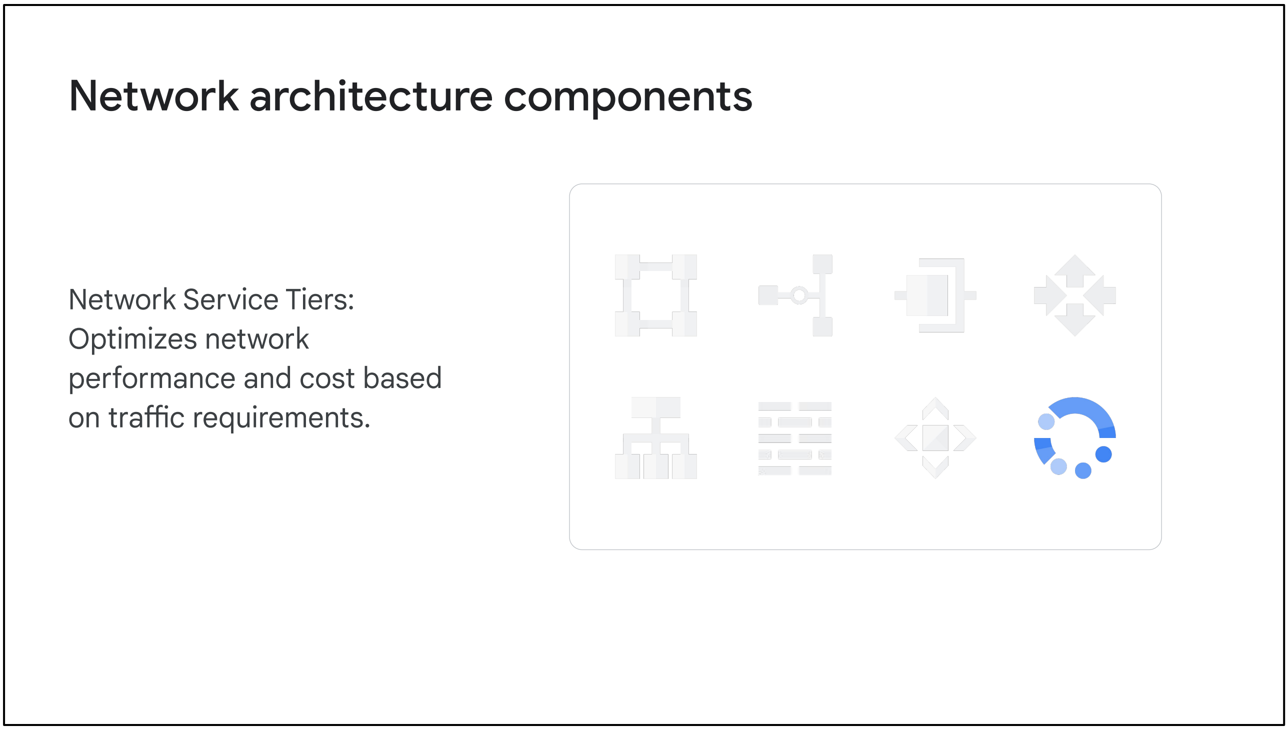
Firewall rules provide granular access control, which is critical in protecting your VPC network. Grouping firewall rules into firewall policies helps you protect your Google Cloud infrastructure more easily. The firewall provides more specific control over traffic entering or leaving individual virtual machine instances.



Network architecture components

Cloud CDN: Cache content using Google's global edge network, accelerating web applications.

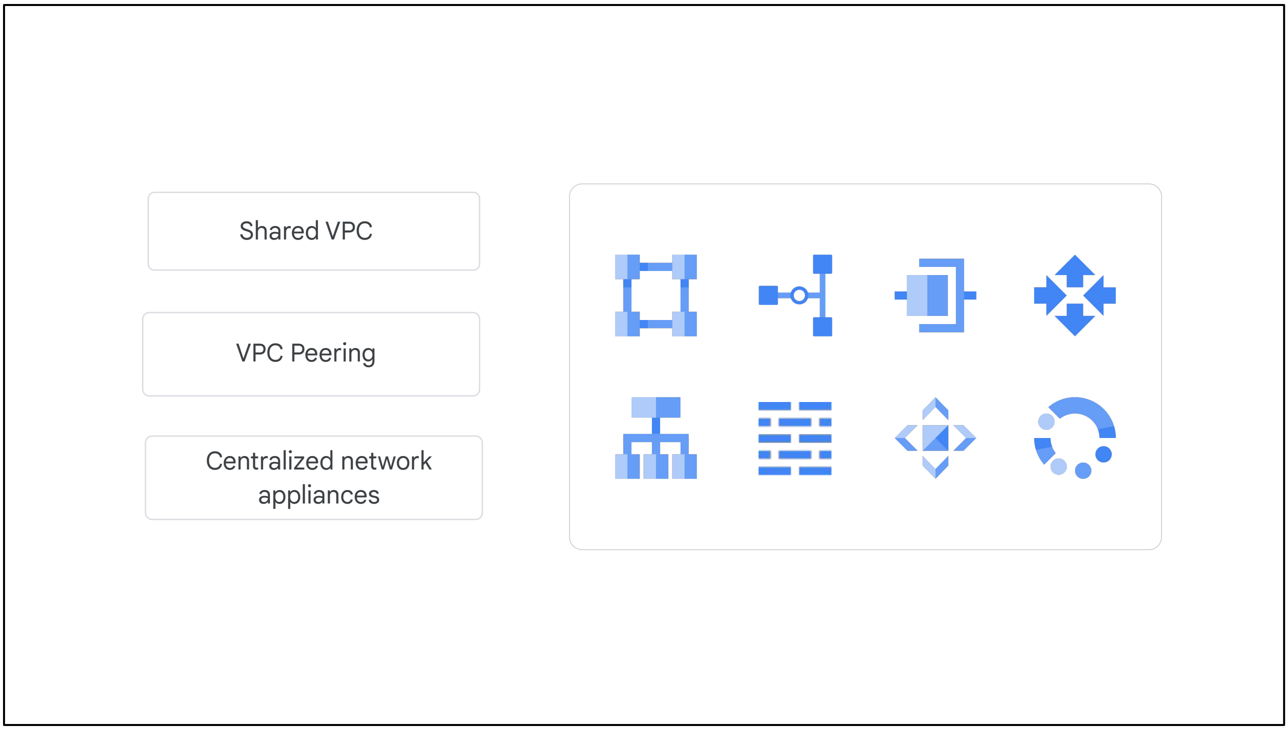
Cloud CDN caches content using Google's global edge network, accelerating web applications.



Network architecture components

Network Service Tiers: Optimizes network performance and cost based on traffic requirements.

By selecting the most appropriate Network Service Tier, you can optimize network performance and cost based on your specific traffic requirements. Choose Standard Tier for general workloads when speed is not a primary concern. Choose Premium Tier for demanding applications that require higher throughput and lower latency.



Shared VPC

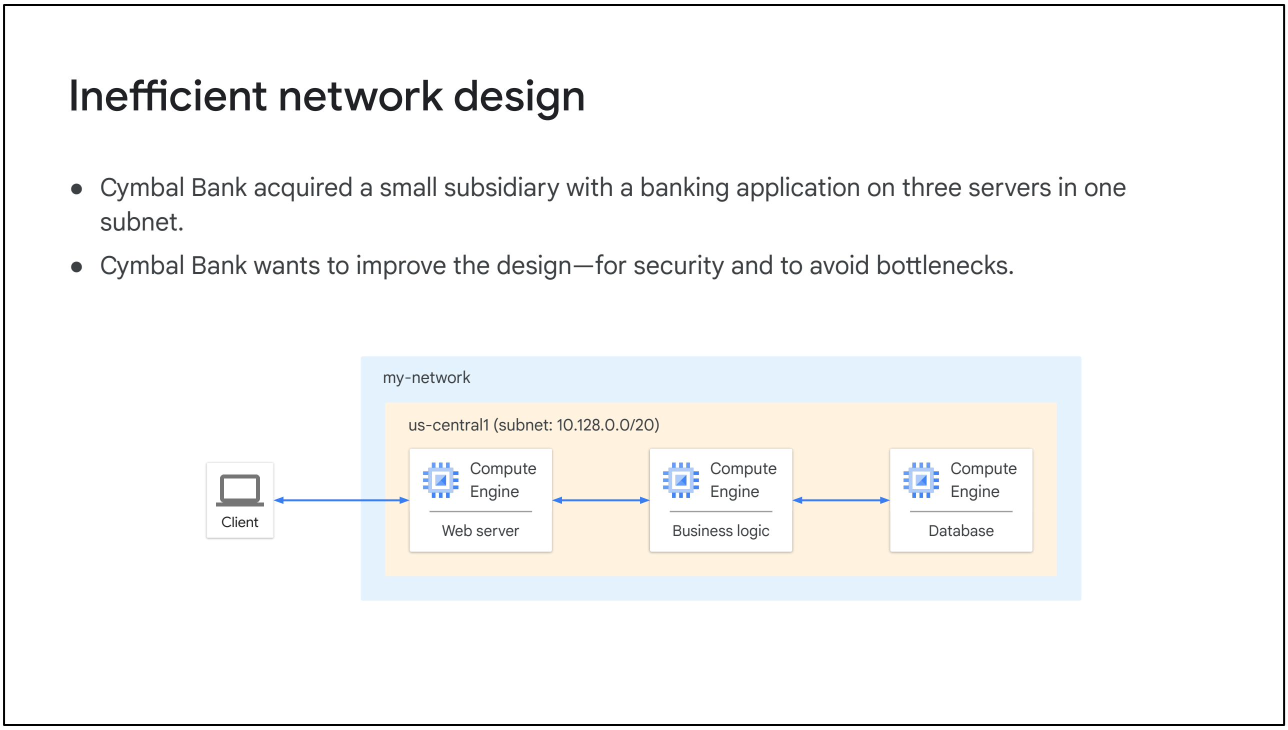
VPC Peering

Centralized network appliances

Shared VPC enables you to share VPC networks across different projects. You can use Shared VPC to simplify network management and resource consolidation, with streamlined network configuration and access control management. Clients can communicate over the Shared VPC network using internal IP addresses.

VPC Network Peering enables you to connect VPC networks within a single project or across organizations while providing control over route exchange. As with Shared VPC, clients using VPC network peering communicate using internal IP addresses.

Simplify your network management by using centralized appliances to carry out essential network functions. Common appliances include intrusion protection systems, web application firewalls (WAFs), and load balancers. These network appliances can be used to enhance the features and protection provided directly by Google Cloud.

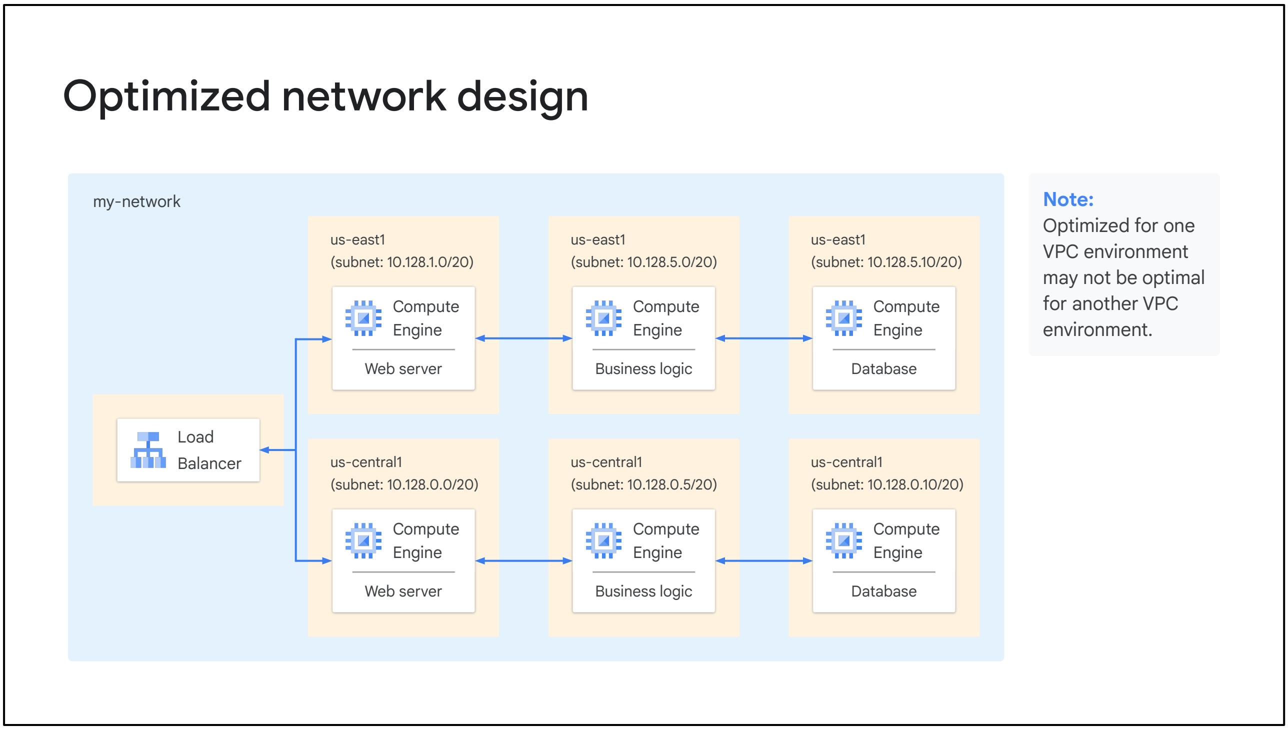


Inefficient network design

- Cymbal Bank acquired a small subsidiary with a banking application on three servers in one subnet.
- Cymbal Bank wants to improve the design—for security and to avoid bottlenecks.

Cymbal Bank acquired a small subsidiary with a banking application on three VMs in one subnet. One VM will host the web server, another VM will host the business logic, and another VM will host the database.

This approach was fine but now Cymbal Bank wants to roll out this banking application to a global audience, with clients in Asia, North America, and Europe. Cymbal Bank wants to avoid bottlenecks.



Optimized network design

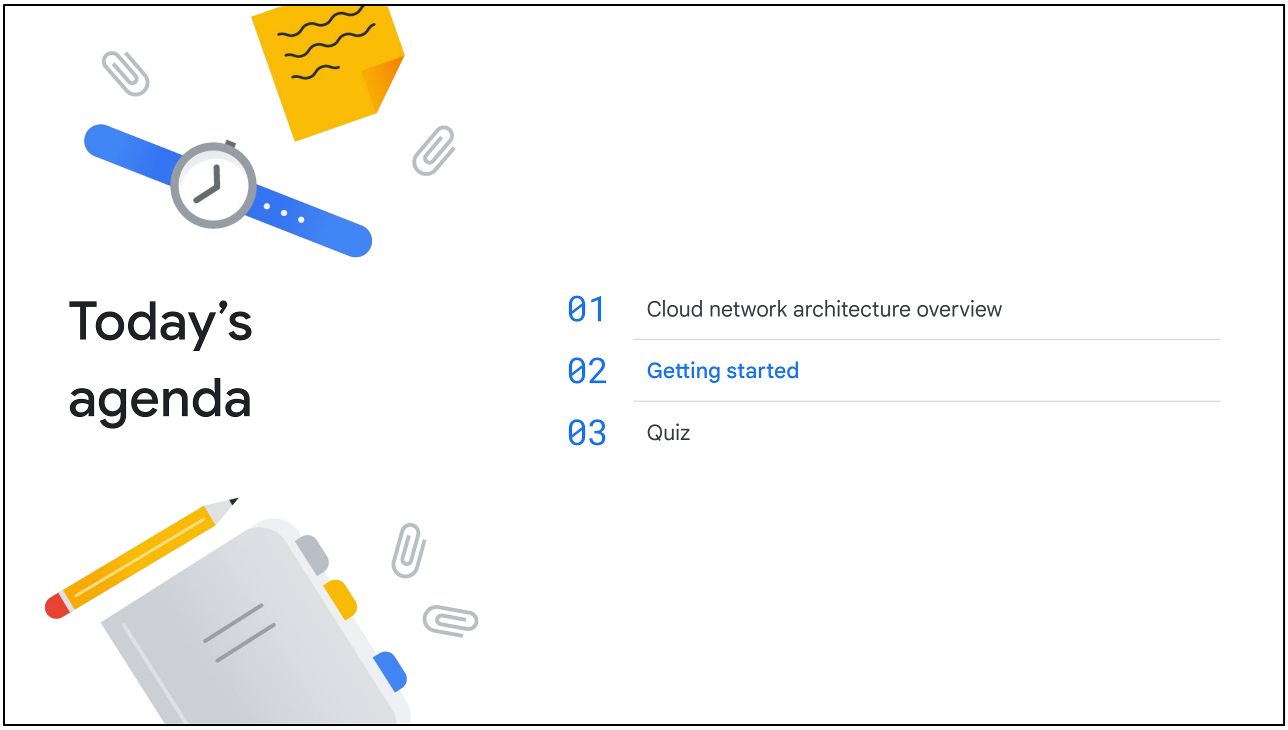
Note:
Optimized for one VPC environment may not be optimal for another VPC environment.

This network design is better for the following reasons:

There are more servers to spread out the processing. Here, we see two sets of VMs that run the web server, the business logic, and the database. Probably, you would use more than two sets of VMs, but only two sets are shown here to make the slide simpler to read. A load balancer handles routing client requests to the least busy set of VMs. This way, you reduce the likelihood of a bottleneck.

Each VM is in a separate subnet. This approach allows you to apply different security—such as firewall rules and IAM permissions—to each subnet. Therefore, to each VM. For example, using this approach, you can lock down the database to only accept messages from the business logic VM.

Depending on the application—and on the clients that use it—there may be other design changes that would be appropriate. For now, it's important to note that a good network design can help make an application run faster and more securely. In this course, you will learn some common network design approaches.



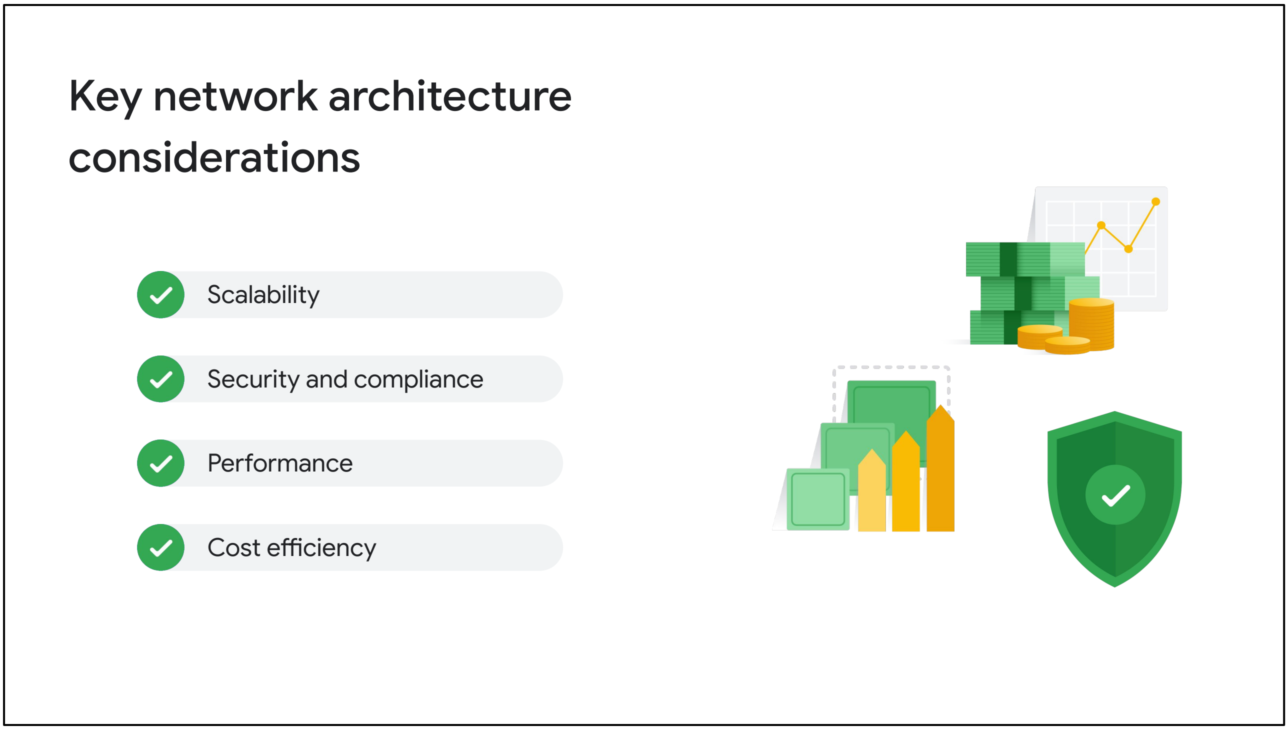
Today's agenda

01 Cloud network architecture overview

02 **Getting started**

03 Quiz

Next, let's briefly discuss some key considerations to design network architecture.



Key network architecture considerations

- ✓ Scalability
- ✓ Security and compliance
- ✓ Performance
- ✓ Cost efficiency

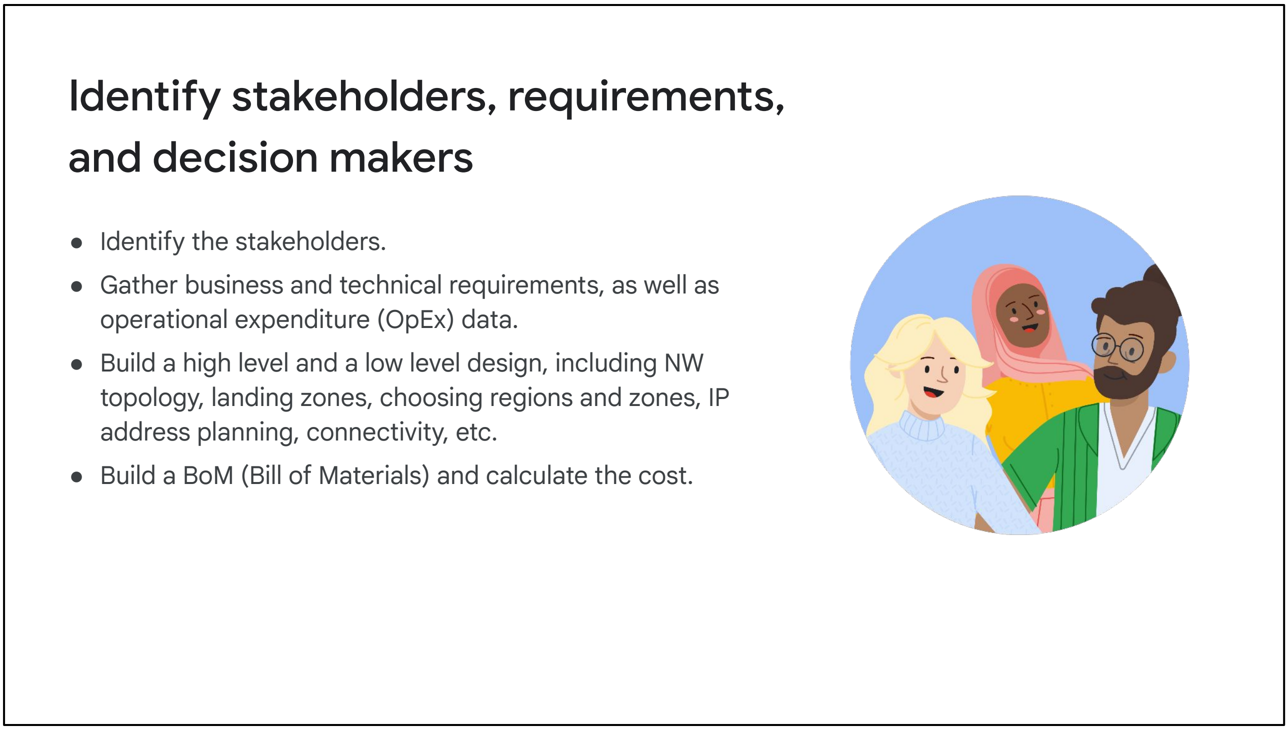
When designing a network architecture, there are a number of key considerations. These include scalability, security, performance, and cost efficiency.

Scalability refers to the ability of your network to accommodate increasing demands, whether it's adding more resources or handling growing traffic volume.

Security refers to protecting your network from unauthorized access and attacks. Implementing robust security measures like firewalls, access controls, and encryption is crucial to safeguarding your network from unauthorized access, data breaches, and cyberattacks. Compliance refers to observing guidelines, rules, and restrictions of your organization, industry, and pertinent government bodies.

Performance refers to the speed and responsiveness of your network. Optimizing network performance translates to faster data transfer, improved application responsiveness, and a smooth user experience for your applications and services.

Cost efficiency refers to the cost of designing, implementing, and operating your network. Striking a balance between achieving your network goals and staying within budget is essential. Google Cloud offers various cost-optimization strategies and tools to help you build a cost-effective network architecture.



Identify stakeholders, requirements, and decision makers

- Identify the stakeholders.
- Gather business and technical requirements, as well as operational expenditure (OpEx) data.
- Build a high level and a low level design, including NW topology, landing zones, choosing regions and zones, IP address planning, connectivity, etc.
- Build a BoM (Bill of Materials) and calculate the cost.

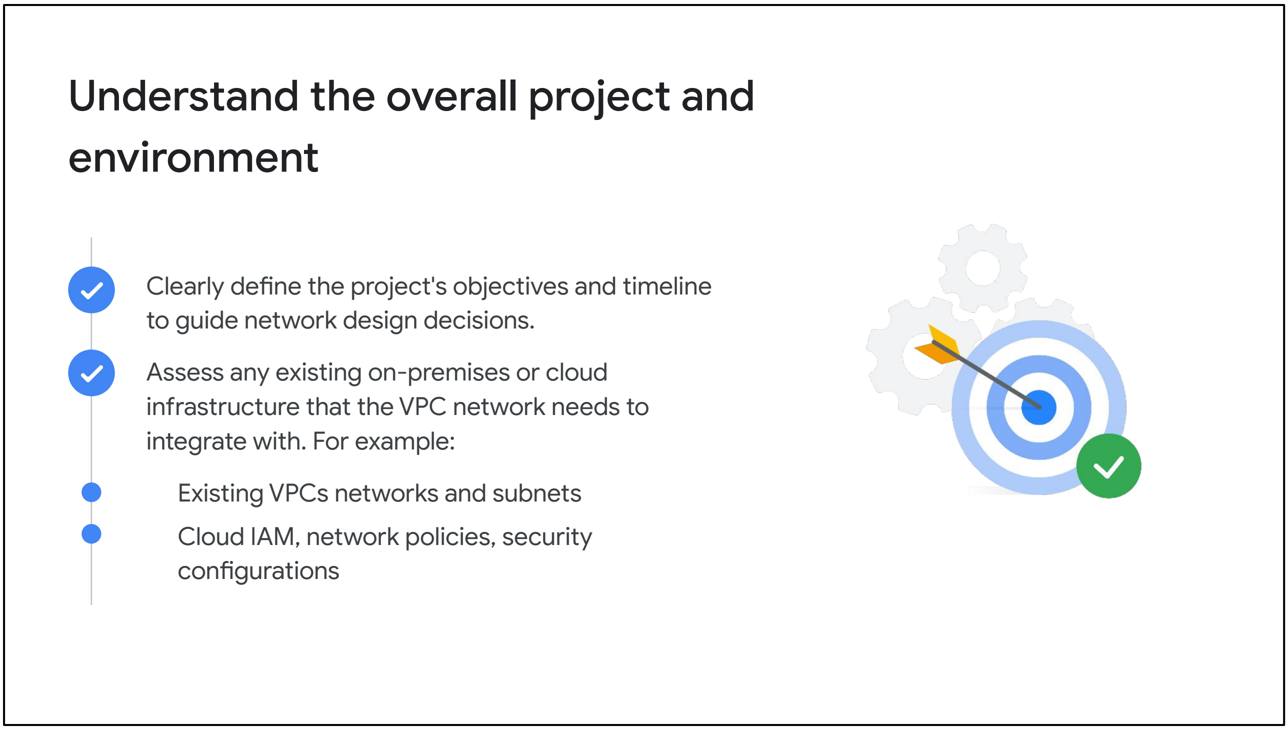
As a first step in your VPC network design, identify the decision makers and stakeholders that you must satisfy. Stakeholders might include application owners, security architects, solution architects, and operations managers. The stakeholders themselves might change depending on whether you are planning your VPC network for a project, a line of business, or the entire organization.

Gather requirements. Engage with stakeholders to understand their specific needs regarding security, performance, scalability, compliance, and budget. This also includes the operational expenditure. This work might involve conducting interviews, workshops, or reviewing existing documentation. You also must identify the people within your organization that can make decisions to approve your network design. For example, engineering managers and accounting personnel.

With a clear understanding of the requirements, we can now begin to translate them into a tangible network design. The high-level design outlines the overall structure of the network, including the major components and their relationships. The low-level design provides a more granular view, specifying device configurations, IP addressing schemes, and security protocols. This phase also involves making critical decisions about cloud infrastructure, geographic locations, and connectivity options.

Finally, build a BoM (Bill of Materials) and calculate the cost. This comprehensive list includes all hardware, software, licenses, and services required to implement the network. It serves as the basis for calculating the total cost of the project, both in terms of upfront capital expenditures (CapEx) and ongoing operational expenditures

(OpEx). This detailed cost analysis allows stakeholders to make informed decisions about the network design and implementation.

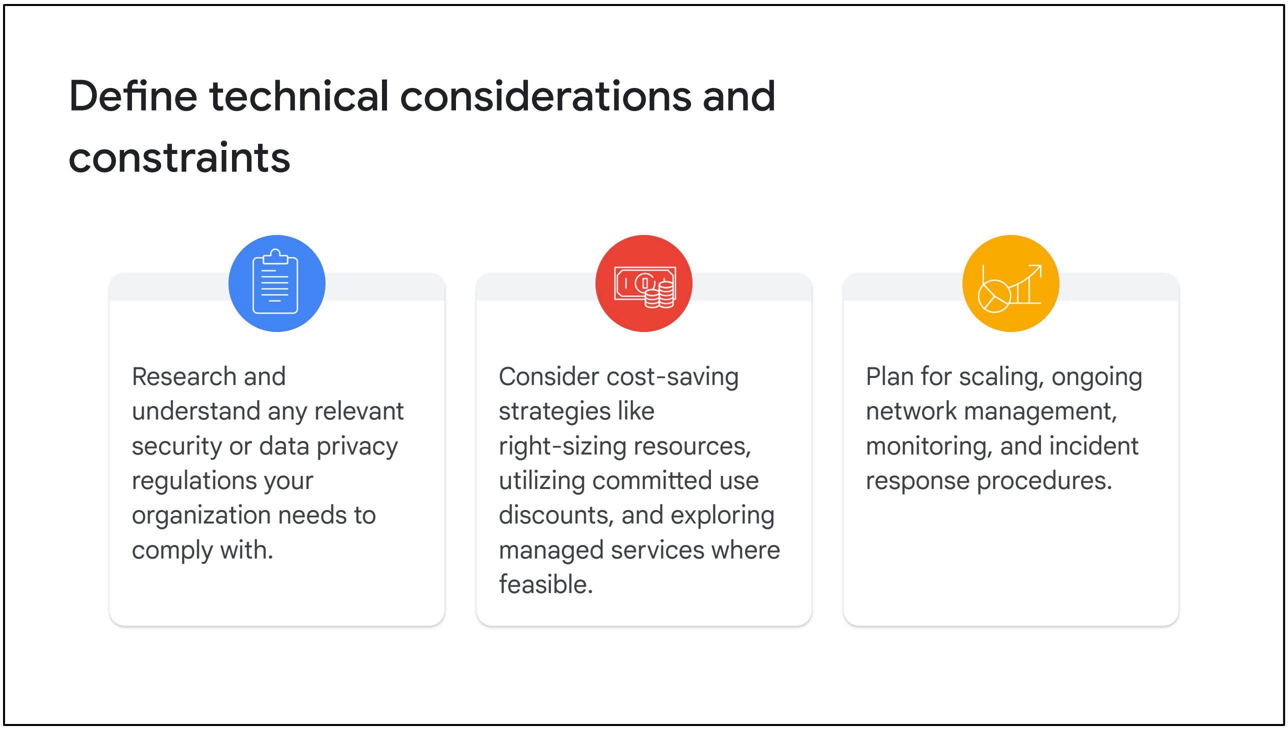


Understand the overall project and environment

- ✓ Clearly define the project's objectives and timeline to guide network design decisions.
- ✓ Assess any existing on-premises or cloud infrastructure that the VPC network needs to integrate with. For example:
  - Existing VPCs networks and subnets
  - Cloud IAM, network policies, security configurations

Clearly define the project's objectives and timeline to guide network design decisions. This helps determine resource allocation, architecture complexity, and implementation phases.

Assess any existing on-premises or cloud infrastructure that the VPC network needs to integrate with. This includes identifying existing VPCs, subnets, security configurations, Cloud IAM, and network policies.



Define technical considerations and constraints

Research and understand any relevant security or data privacy regulations your organization needs to comply with.

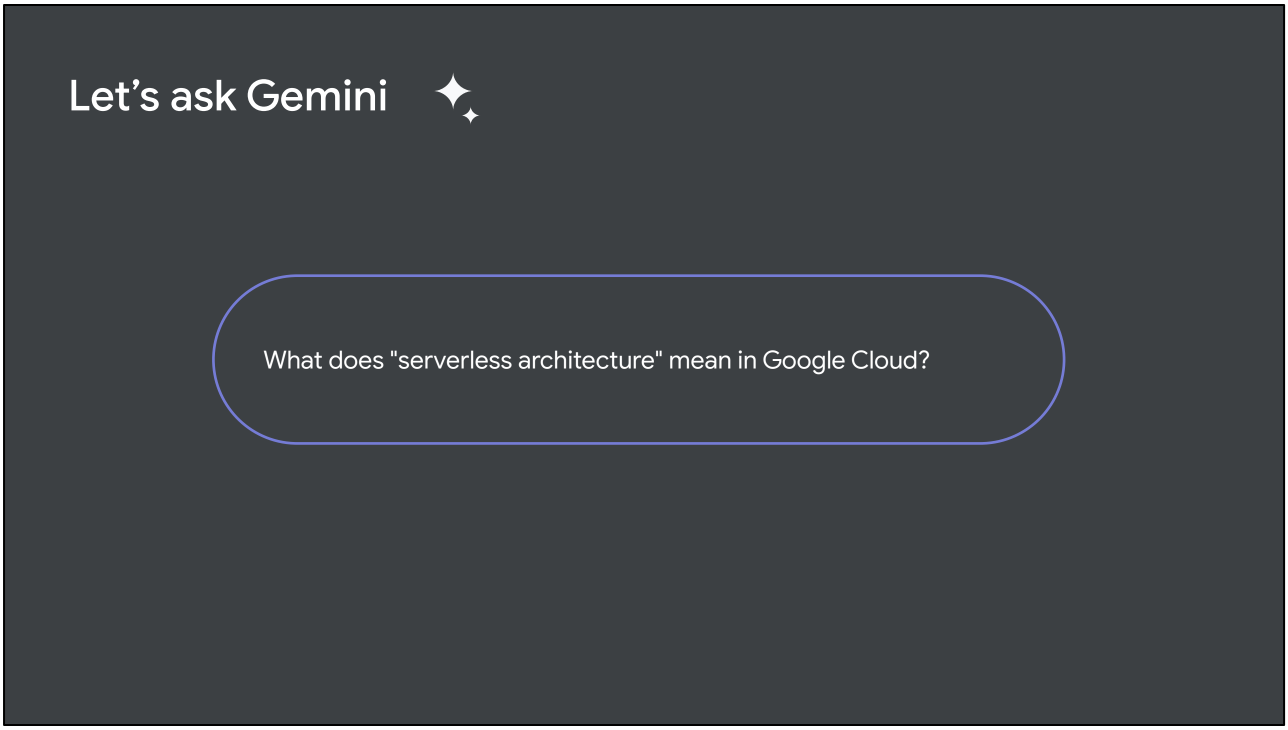
Consider cost-saving strategies like right-sizing resources, utilizing committed use discounts, and exploring managed services where feasible.

Plan for scaling, ongoing network management, monitoring, and incident response procedures.

Research and understand any relevant security or data privacy regulations your organization needs to follow. This might influence aspects like data segregation, access control, and logging.

Consider cost-saving strategies like right-sizing resources, utilizing committed use discounts, and exploring managed services where feasible.

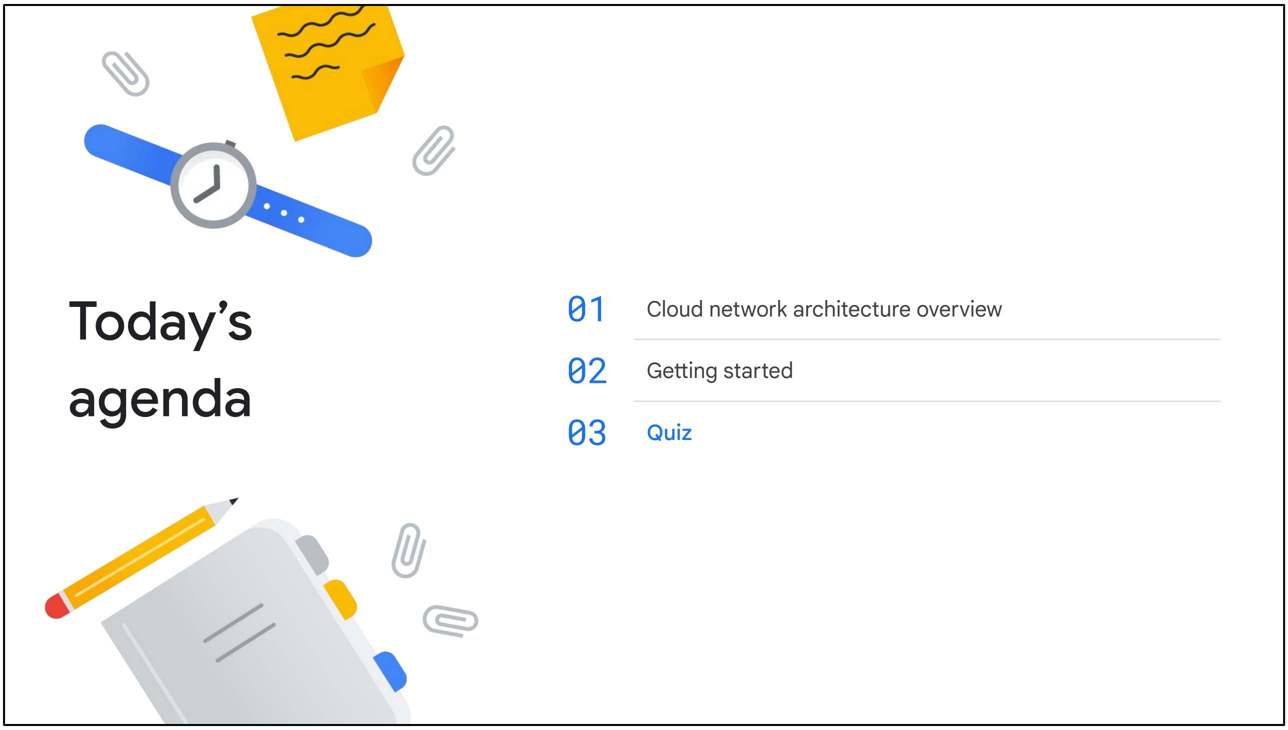
Plan for ongoing network management, monitoring, and incident response procedures. This might involve defining roles and responsibilities, automation practices, and logging configurations.



Let’s ask Gemini

What does "serverless architecture" mean in Google Cloud?

Let’s take a look at an example of how you can use Gemini to help you learn more about network architecture..
You can explore your options by asking Gemini: “What does serverless architecture mean in Google Cloud”?



Today's agenda

01 Cloud network architecture overview

02 Getting started

03 Quiz

Next, let's test your knowledge about this lecture.

Quiz | Question 1

Question

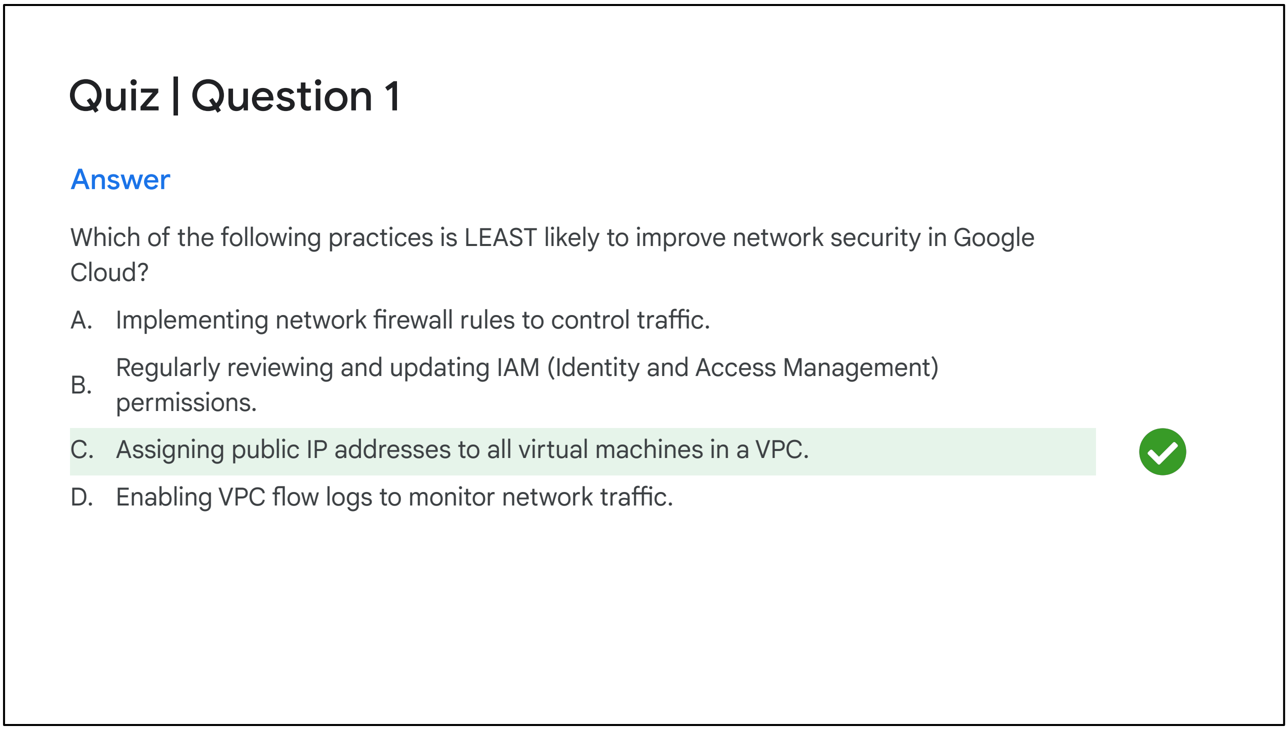
Which of the following practices is LEAST likely to improve network security in Google Cloud?

A. Implementing network firewall rules to control traffic.

B. Regularly reviewing and updating IAM (Identity and Access Management) permissions.

C. Assigning public IP addresses to all virtual machines in a VPC.

D. Enabling VPC flow logs to monitor network traffic.



Quiz | Question 1

Answer

Which of the following practices is LEAST likely to improve network security in Google Cloud?

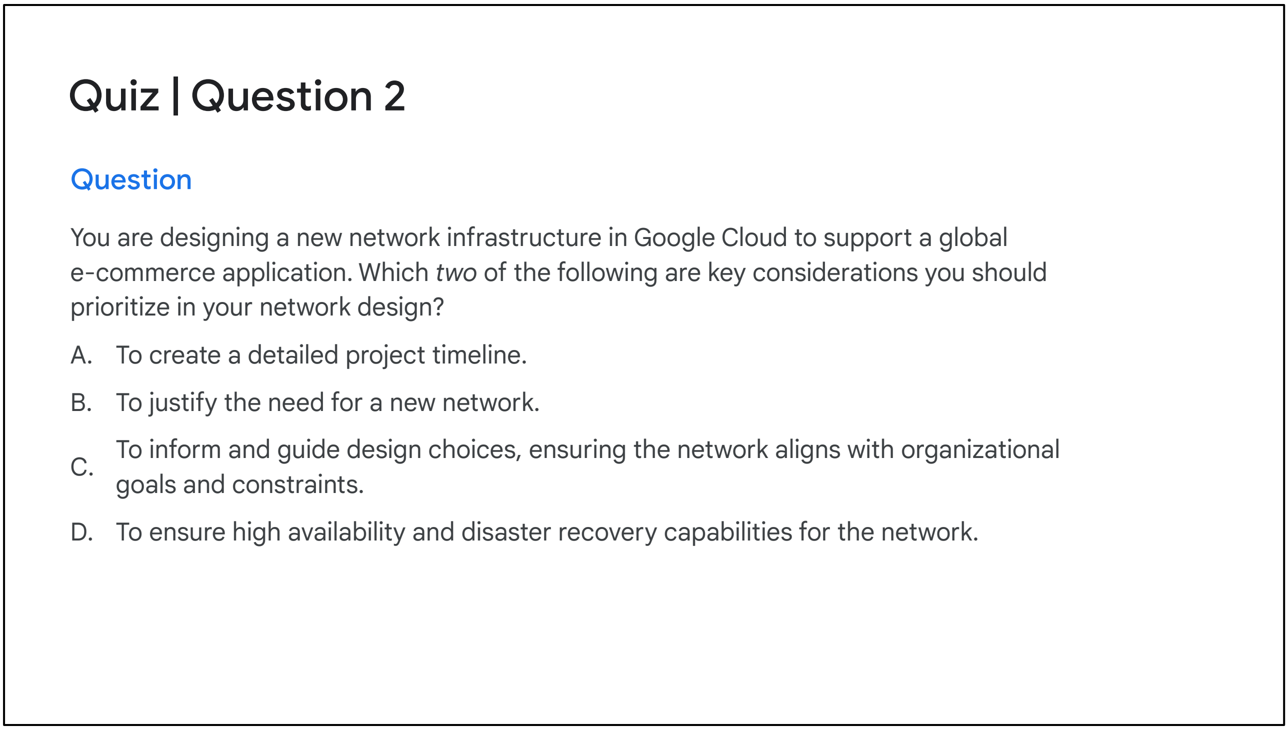
A. Implementing network firewall rules to control traffic.

B. Regularly reviewing and updating IAM (Identity and Access Management) permissions.

C. Assigning public IP addresses to all virtual machines in a VPC. ✓

D. Enabling VPC flow logs to monitor network traffic.

Assigning public IP addresses to all virtual machines in a VPC is considered a security risk because it directly exposes those instances to the public internet. This makes them potential targets for malicious actors who could attempt unauthorized access, data breaches, or denial-of-service attacks.



Quiz | Question 2

Question

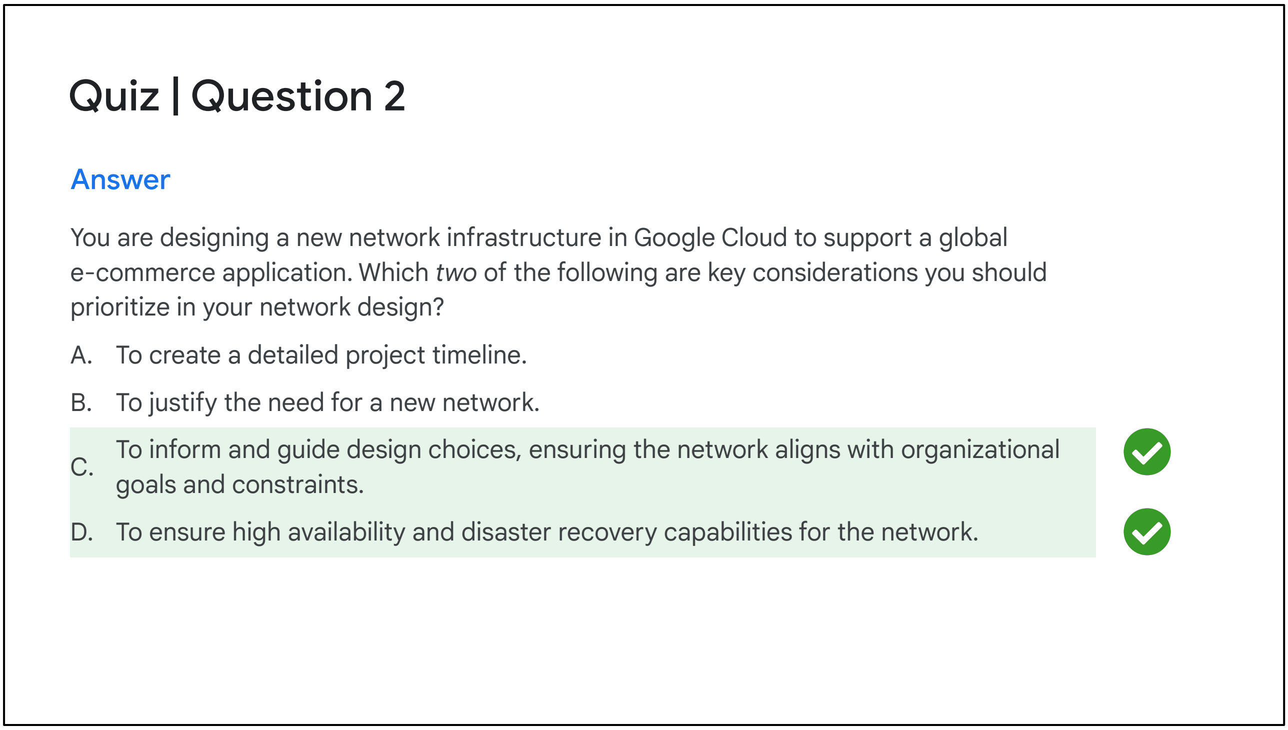
You are designing a new network infrastructure in Google Cloud to support a global e-commerce application. Which *two* of the following are key considerations you should prioritize in your network design?

A. To create a detailed project timeline.

B. To justify the need for a new network.

C. To inform and guide design choices, ensuring the network aligns with organizational goals and constraints.

D. To ensure high availability and disaster recovery capabilities for the network.



Quiz | Question 2

Answer

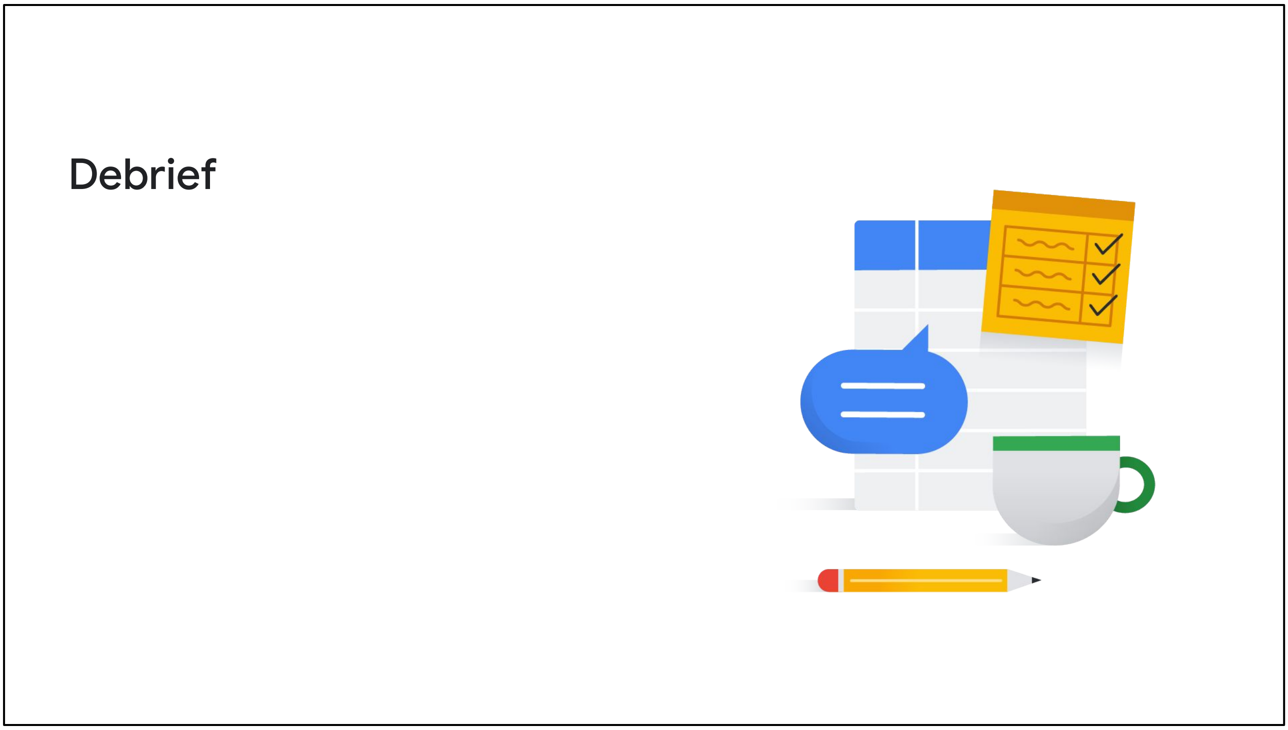
You are designing a new network infrastructure in Google Cloud to support a global e-commerce application. Which *two* of the following are key considerations you should prioritize in your network design?

A. To create a detailed project timeline.

B. To justify the need for a new network.

C. To inform and guide design choices, ensuring the network aligns with organizational goals and constraints. ✓

D. To ensure high availability and disaster recovery capabilities for the network. ✓



Debrief

In this module, you were introduced to the concept of network architecture and why it is important for optimal functioning of your Google Cloud environments. You learned about some important design concerns, core design components, and how to get started planning a network architecture.

Thank you.