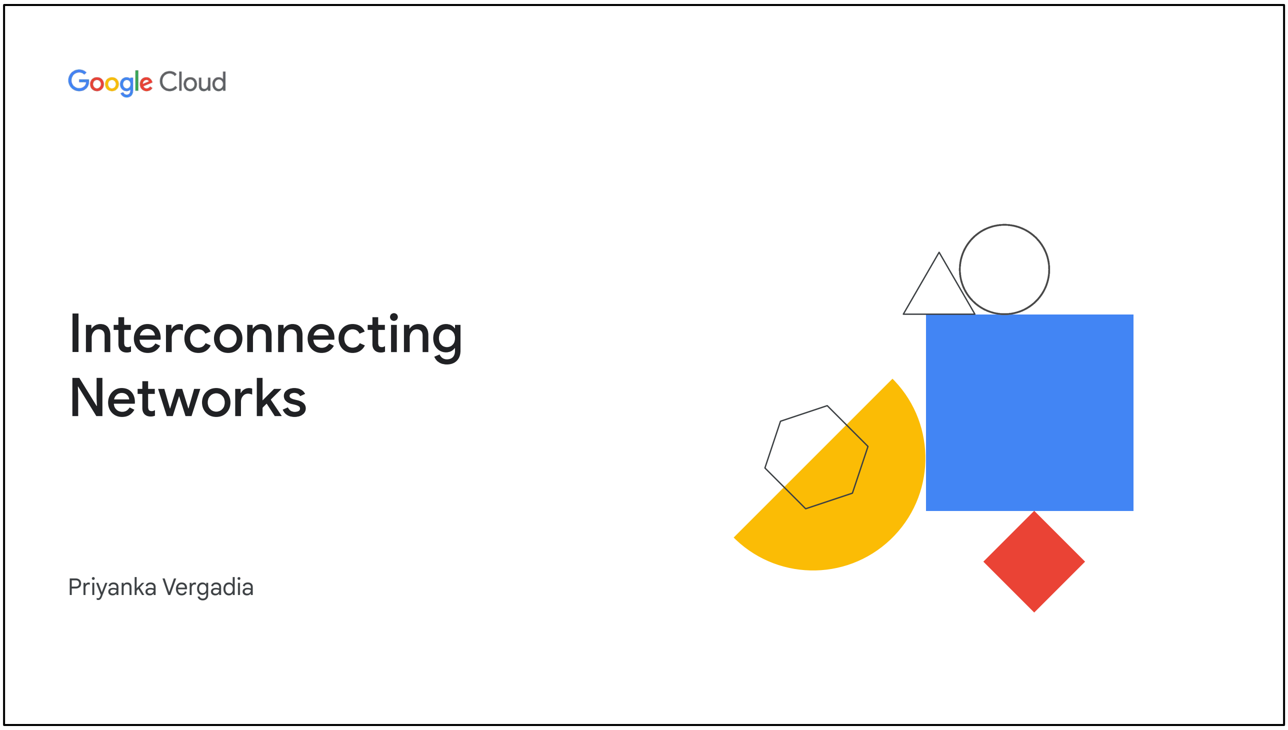
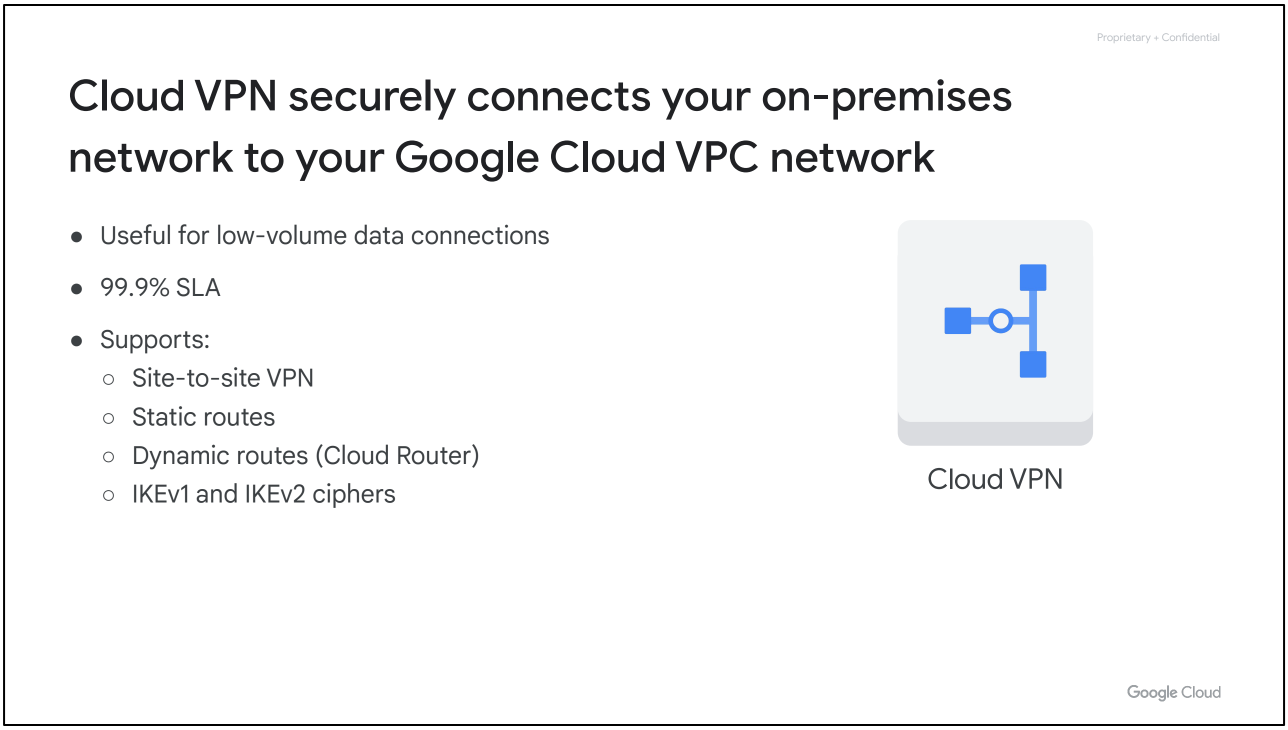


Interconnecting Networks

Priyanka Vergadia

Hi I’m Priyanka Vergadia, a developer advocate for Google Cloud. In this module, we focus on Interconnecting Networks.

Different applications and workloads require different network connectivity solutions. That is why Google supports multiple ways to connect your infrastructure to GCP.



Cloud VPN securely connects your on-premises network to your Google Cloud VPC network

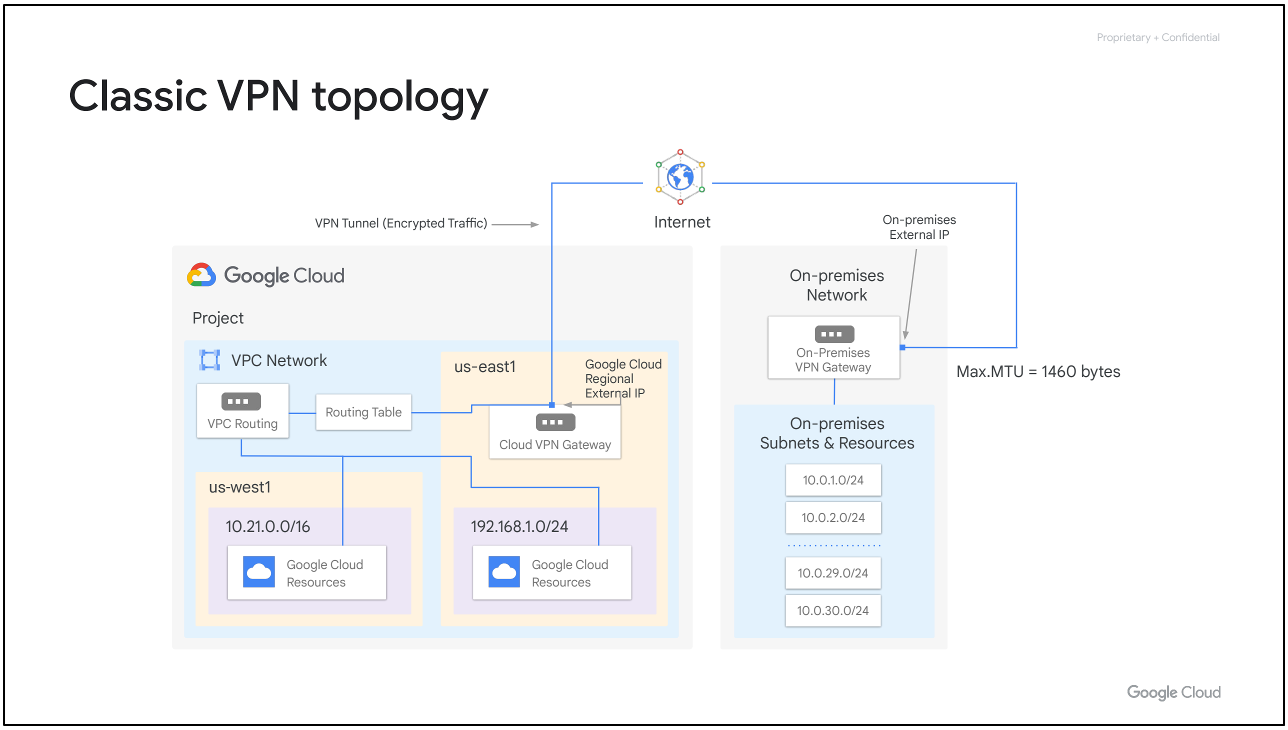
- Useful for low-volume data connections
- 99.9% SLA
- Supports:
  - Site-to-site VPN
  - Static routes
  - Dynamic routes (Cloud Router)
  - IKEv1 and IKEv2 ciphers

Cloud VPN

Cloud VPN securely connects your on-premises network to your Google Cloud VPC network through an IPsec VPN tunnel. Traffic traveling between the two networks is encrypted by one VPN gateway, then decrypted by the other VPN gateway. This protects your data as it travels over the public internet, and that's why Cloud VPN is useful for low-volume data connections.

As a managed service, Cloud VPN provides an SLA of 99.9% service availability and supports site-to-site VPN, static and dynamic routes, and IKEv1 and IKEv2 ciphers. Cloud VPN doesn't support use cases where client computers need to “dial in” to a VPN using client VPN software. Also, dynamic routes are configured with Cloud Router, which we will cover briefly.

For more information about the SLA and these features, please refer to the documentation. https://cloud.google.com/vpn/docs/concepts/overview



Classic VPN topology

Internet

VPN Tunnel (Encrypted Traffic)

On-premises External IP

Google Cloud

Project

VPC Network

VPC Routing

Routing Table

us-east1

Google Cloud Regional External IP

Cloud VPN Gateway

us-west1

10.21.0.0/16

Google Cloud Resources

192.168.1.0/24

Google Cloud Resources

On-premises Network

On-Premises VPN Gateway

Max.MTU = 1460 bytes

On-premises Subnets & Resources

10.0.1.0/24

10.0.2.0/24

10.0.29.0/24

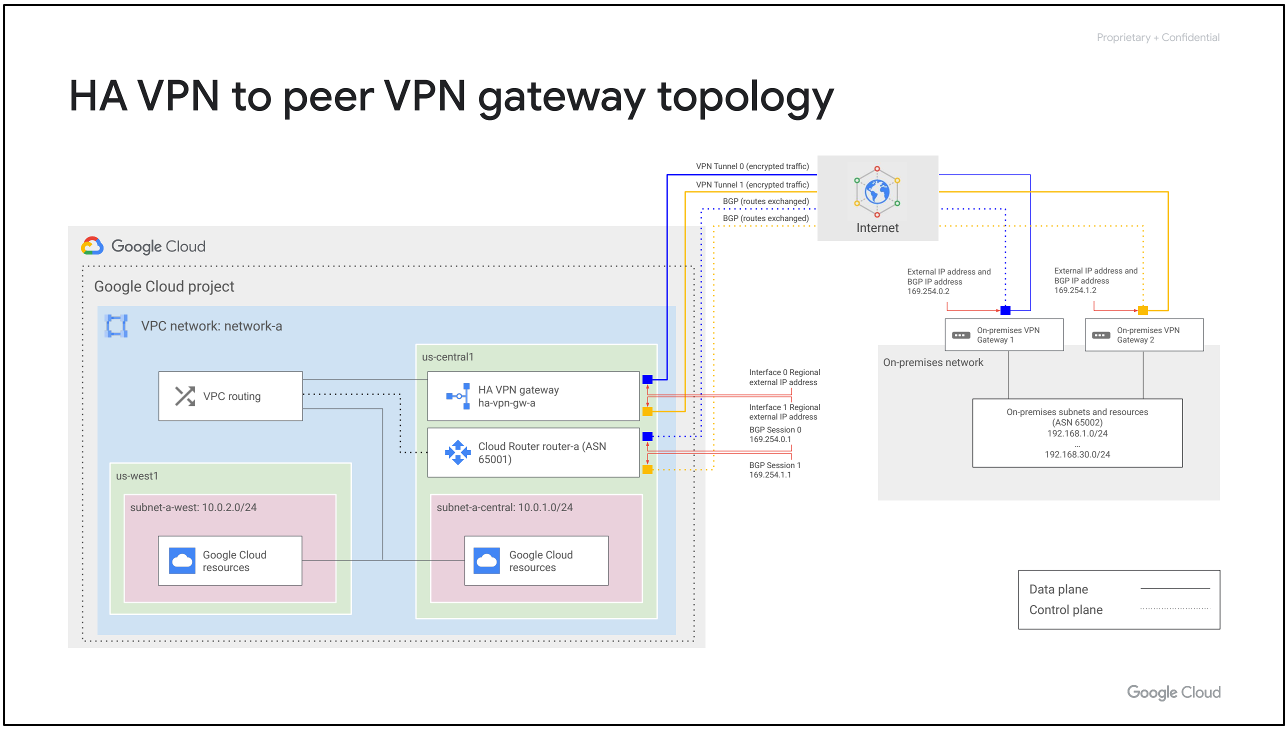
10.0.30.0/24

Let me walk through an example of Cloud VPN. This diagram shows a Classic VPN connection between your VPC and on-premises network. Your VPC network has subnets in us-east1 and us-west1, with Google Cloud resources in each of those regions. These resources are able to communicate using their internal IP addresses because routing within a network is automatically configured (assuming that firewall rules allow the communication).

Now, in order to connect to your on-premises network and its resources, you need to configure your Cloud VPN gateway, on-premises VPN gateway, and two VPN tunnels. The Cloud VPN gateway is a regional resource that uses a regional external IP address.

Your on-premises VPN gateway can be a physical device in your data center or a physical or software-based VPN offering in another cloud provider's network. This VPN gateway also has an external IP address.

A VPN tunnel then connects your VPN gateways and serves as the virtual medium through which encrypted traffic is passed. In order to create a connection between two VPN gateways, you must establish two VPN tunnels. Each tunnel defines the connection from the perspective of its gateway, and traffic can only pass when the pair of tunnels is established.



HA VPN to peer VPN gateway topology

Google Cloud

Google Cloud project

VPC network: network-a

VPC routing

us-central1

HA VPN gateway
ha-vpn-gw-a

Cloud Router router-a (ASN 65001)

us-west1

subnet-a-west: 10.0.2.0/24

Google Cloud resources

subnet-a-central: 10.0.1.0/24

Google Cloud resources

VPN Tunnel 0 (encrypted traffic)

VPN Tunnel 1 (encrypted traffic)

BGP (routes exchanged)

BGP (routes exchanged)

Internet

Interface 0 Regional external IP address

Interface 1 Regional external IP address

BGP Session 0
169.254.0.1

BGP Session 1
169.254.1.1

External IP address and BGP IP address
169.254.0.2

External IP address and BGP IP address
169.254.1.2

On-premises VPN Gateway 1

On-premises VPN Gateway 2

On-premises network

On-premises subnets and resources
(ASN 65002)
192.168.1.0/24
...
192.168.30.0/24

Data plane

Control plane

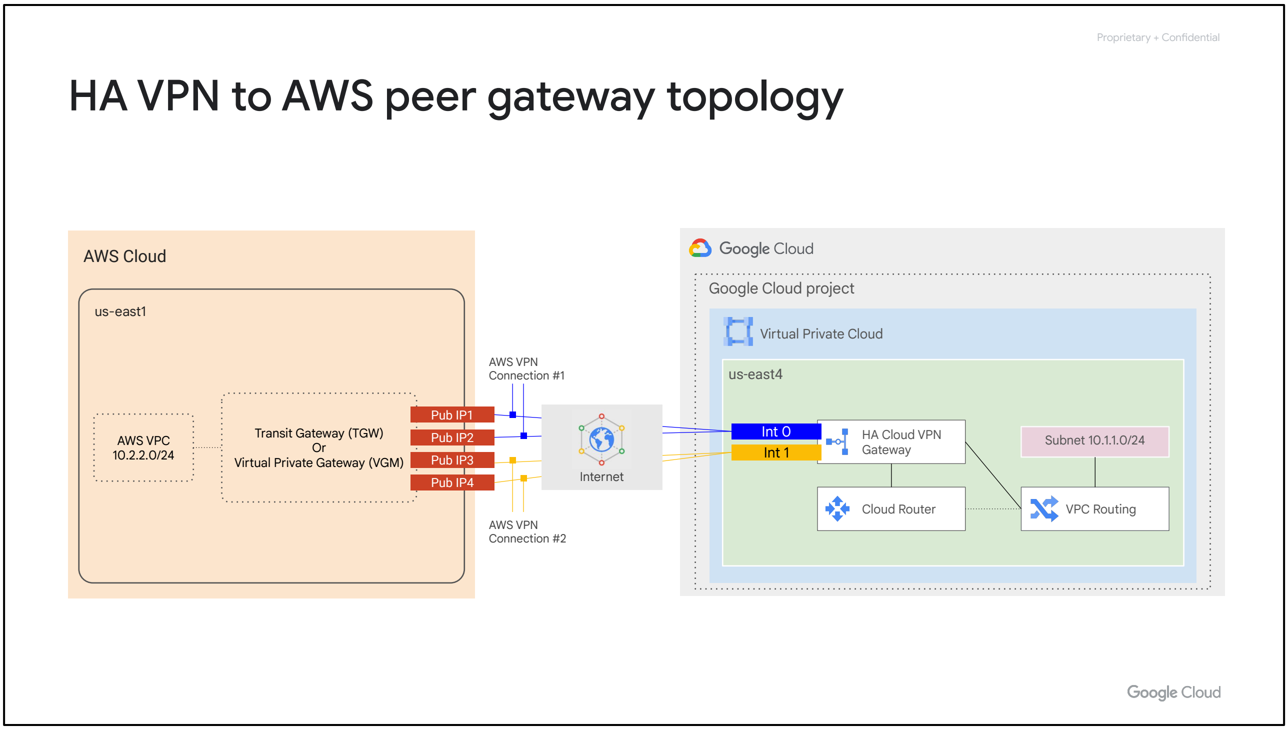
Google Cloud

There are three typical peer gateway configurations for HA VPN. An HA VPN gateway to two separate peer VPN devices, each with its own IP address, an HA VPN gateway to one peer VPN device that uses two separate IP addresses and an HA VPN gateway to one peer VPN device that uses one IP address.

Let's walk through an example. In this topology, one HA VPN gateway connects to two peer devices. Each peer device has one interface and one external IP address. The HA VPN gateway uses two tunnels, one tunnel to each peer device. If your peer-side gateway is hardware-based, having a second peer-side gateway provides redundancy and failover on that side of the connection.

A second physical gateway lets you take one of the gateways offline for software upgrades or other scheduled maintenance. It also protects you if there is a failure in one of the devices.

In Google Cloud, the REDUNDANCY_TYPE for this configuration takes the value TWO_IPS_REDUNDANCY. The example shown here provides 99.99% availability.



Proprietary + Confidential

HA VPN to AWS peer gateway topology

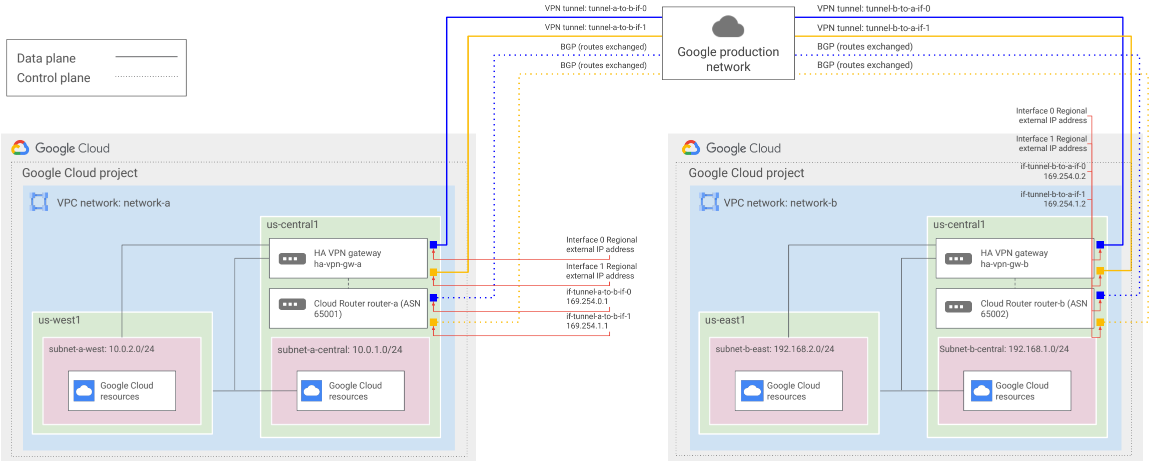
Google Cloud

When configuring an HA VPN external VPN gateway to Amazon Web Services (AWS), you can use either a transit gateway or a virtual private gateway. Only the transit gateway supports equal-cost multipath (ECMP) routing. When enabled, ECMP equally distributes traffic across active tunnels. Let's walk through an example.

In this topology, there are three major gateway components to set up for this configuration. An HA VPN gateway in Google Cloud with two interfaces, two AWS virtual private gateways, which connect to your HA VPN gateway, and an external VPN gateway resource in Google Cloud that represents your AWS virtual private gateway. This resource provides information to Google Cloud about your AWS gateway. The supported AWS configuration uses a total of four tunnels. Two tunnels from one AWS virtual private gateway to one interface of the HA VPN gateway, and two tunnels from the other AWS virtual private gateway to the other interface of the HA VPN gateway.

Proprietary + Confidential

HA VPN between Google Cloud networks topology

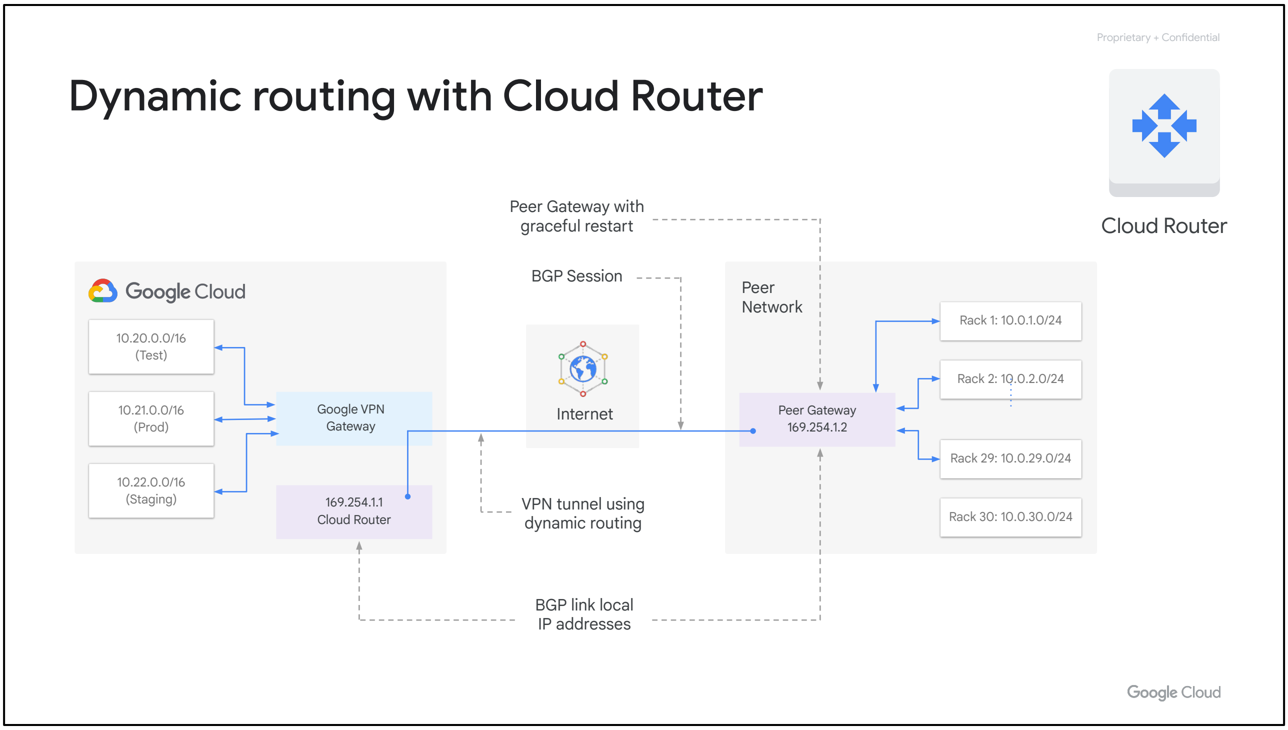

Data plane
Control plane
VPN tunnel: tunnel-a-to-b-if-0
VPN tunnel: tunnel-a-to-b-if-1
BGP (routes exchanged)
BGP (routes exchanged)
Google production network
VPN tunnel: tunnel-b-to-a-if-0
VPN tunnel: tunnel-b-to-a-if-1
BGP (routes exchanged)
BGP (routes exchanged)
Google Cloud
Google Cloud project
VPC network: network-a
us-central1
HA VPN gateway ha-vpn-gw-a
Cloud Router router-a (ASN 65001)
us-west1
subnet-a-west: 10.0.2.0/24
Google Cloud resources
subnet-a-central: 10.0.1.0/24
Google Cloud resources
Interface 0 Regional external IP address
Interface 1 Regional external IP address
if-tunnel-a-to-b-if-0 169.254.0.1
if-tunnel-a-to-b-if-1 169.254.1.1
Interface 0 Regional external IP address
Interface 1 Regional external IP address
if-tunnel-b-to-a-if-0 169.254.0.2
if-tunnel-b-to-a-if-1 169.254.1.2
Google Cloud
Google Cloud project
VPC network: network-b
us-central1
HA VPN gateway ha-vpn-gw-b
Cloud Router router-b (ASN 65002)
us-east1
subnet-b-east: 192.168.2.0/24
Google Cloud resources
Subnet-b-central: 192.168.1.0/24
Google Cloud resources

Google Cloud

You can connect two Google Cloud VPC networks together by using an HA VPN gateway in each network. The configuration shown provides 99.99% availability. From the perspective of each HA VPN gateway you create two tunnels. You connect `interface 0` on one HA VPN gateway to `interface 0` on the other HA VPN, and `interface 1` on one HA VPN gateway to `interface 1` on the other HA VPN.

For more information on HA VPN and moving to HA VPN, refer to the documentation links in the course resources.

[Cloud VPN topologies:
https://cloud.google.com/network-connectivity/docs/vpn/concepts/topologies]
[Moving to HA VPN:
https://cloud.google.com/network-connectivity/docs/vpn/how-to/moving-to-ha-vpn]



Proprietary + Confidential

Dynamic routing with Cloud Router

Cloud Router

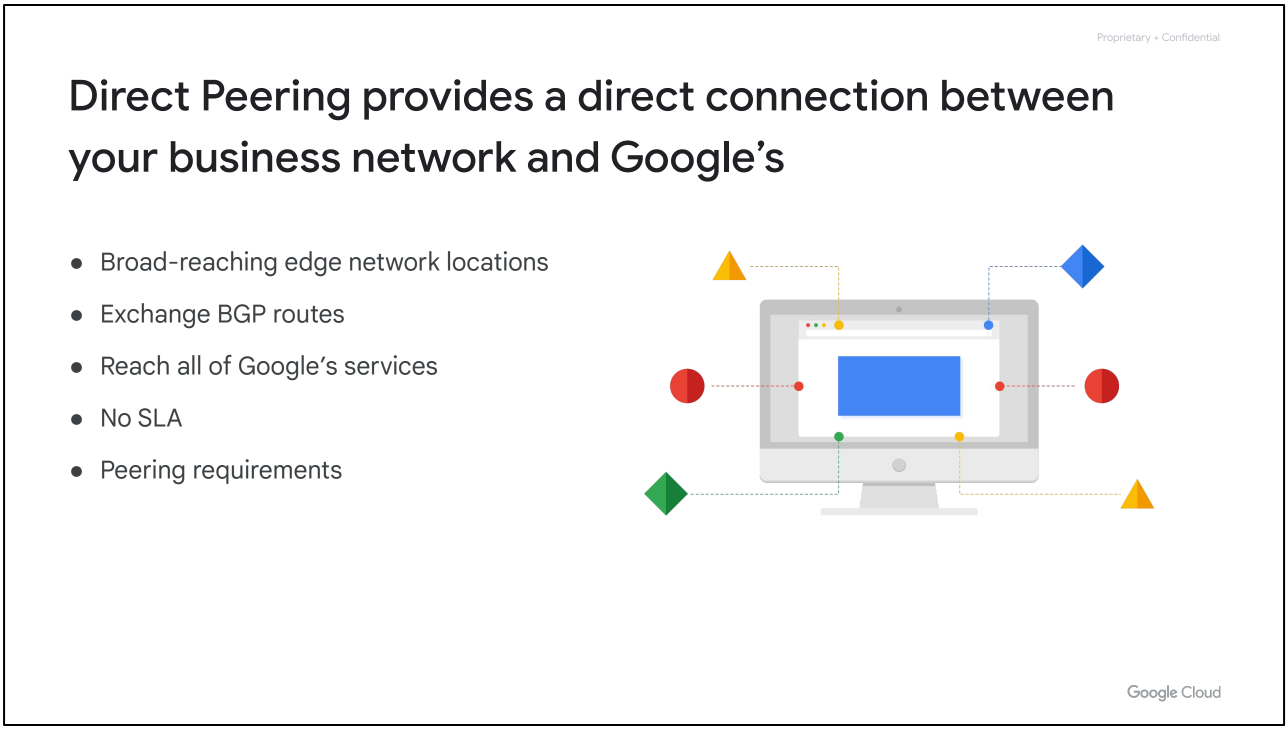
Google Cloud

We mentioned earlier that Cloud VPN supports both static and dynamic routes. In order to use dynamic routes, you need to configure Cloud Routers. Cloud Router can manage routes for a Cloud VPN tunnel using Border Gateway Protocol, or BGP. This routing method allows for routes to be updated and exchanged without changing the tunnel configuration.

For example, this diagram shows two different regional subnets in a VPC network, namely Test and Prod. The on-premises network has 29 subnets, and the two networks are connected through Cloud VPN tunnels. Now, how would you handle adding new subnets? For example, how would you add a new “Staging” subnet in the Google Cloud network and a new on-premises 10.0.30.0/24 subnet to handle growing traffic in your data center?

To automatically propagate network configuration changes, the VPN tunnel uses Cloud Router to establish a BGP session between the VPC and the on-premises VPN gateway, which must support BGP. The new subnets are then seamlessly advertised between networks. This means that instances in the new subnets can start sending and receiving traffic immediately, as you will explore in the upcoming lab.

To set up BGP, an additional IP address has to be assigned to each end of the VPN tunnel. These two IP addresses must be link-local IP addresses, belonging to the IP



Proprietary + Confidential

Direct Peering provides a direct connection between your business network and Google's

- Broad-reaching edge network locations
- Exchange BGP routes
- Reach all of Google's services
- No SLA
- Peering requirements

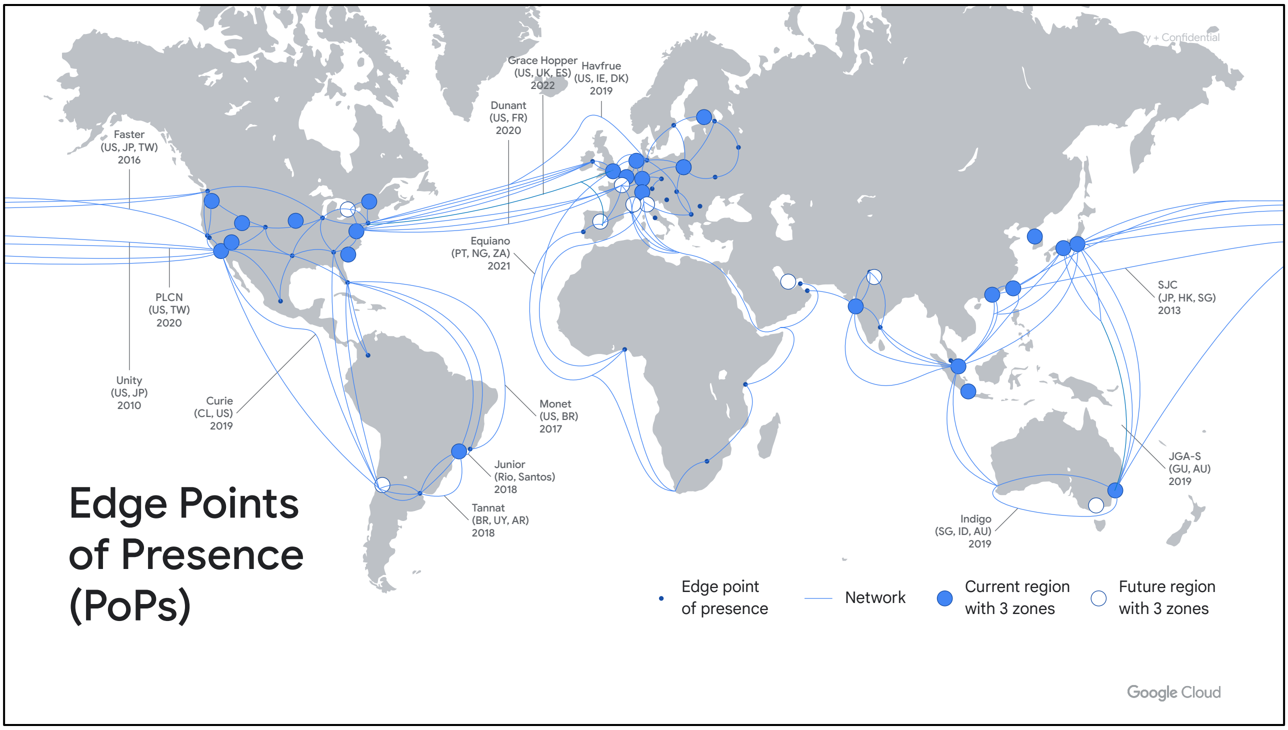
Google Cloud

Let's talk about the Cloud Peering services, which are Direct Peering and Carrier Peering. These services are useful when you require access to Google and Google Cloud properties.

Google allows you to establish a Direct Peering connection between your business network and Google's. With this connection you will be able to exchange internet traffic between your network and Google's at one of Google's broad-reaching edge network locations.

Direct Peering with Google is done by exchanging BGP routes between Google and the peering entity. After a Direct Peering connection is in place, you can use it to reach all of Google's services, including the full suite of Google Cloud Platform products. Unlike Dedicated Interconnect, Direct Peering does not have an SLA.

In order to use Direct Peering, you need to satisfy the peering requirements detailed on this webpage. [https://peering.google.com/#/options/peering].

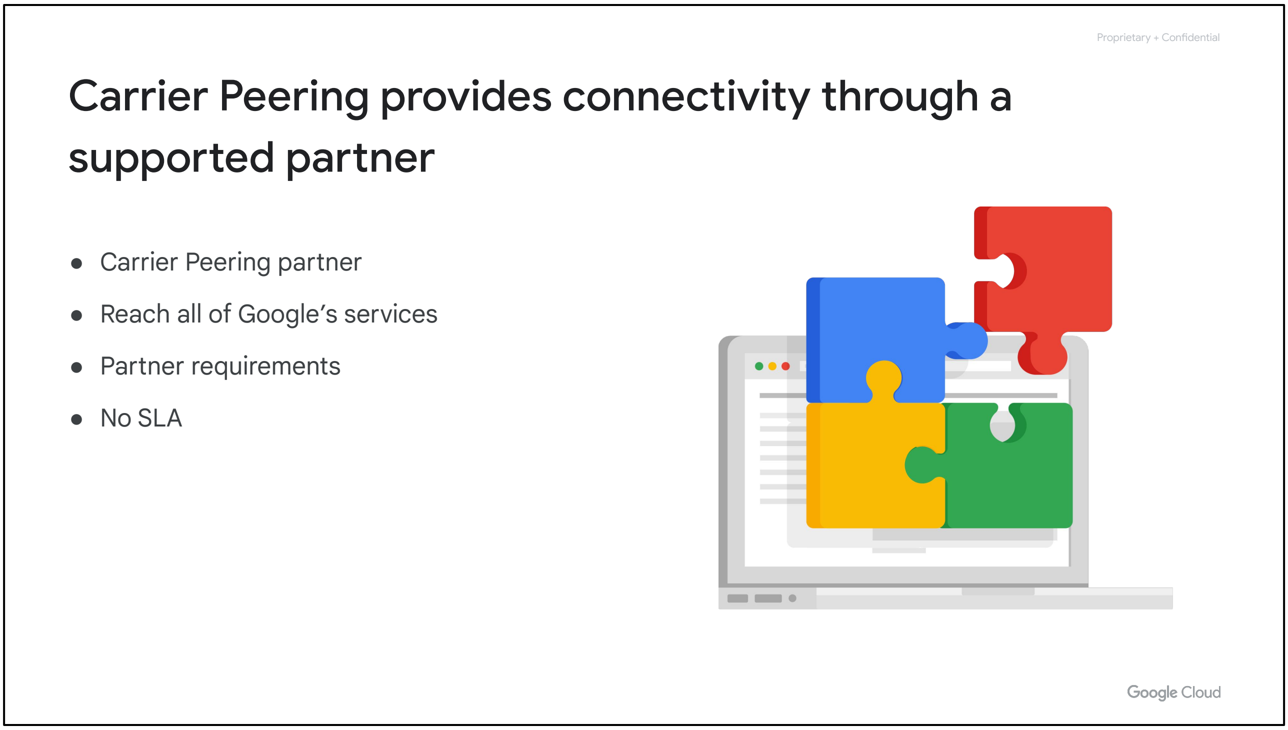


Edge Points of Presence (PoPs)

GCP’s Edge Points of Presence, or PoPs, are where Google's network connects to the rest of the internet via peering. PoPs are present on over 90 internet exchanges and at over 100 interconnection facilities around the world.

For more information about these exchange points and facilities, I recommend looking at Google’s PeeringDB entries, which are linked below this video [https://www.peeringdb.com/asn/15169 and https://www.peeringdb.com/net/4319].

If you look at this map and say “Hey, I am nowhere near one of those locations,” you will want to consider Carrier Peering.

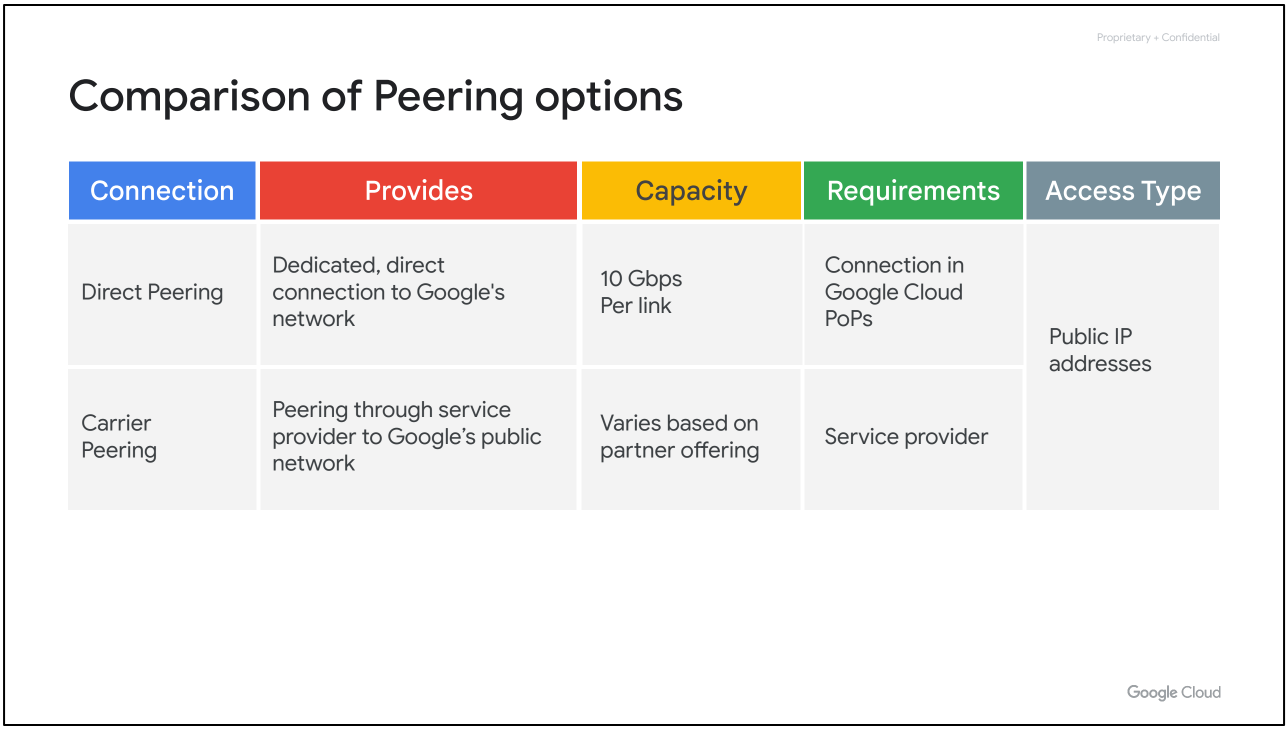


Carrier Peering provides connectivity through a supported partner

- Carrier Peering partner
- Reach all of Google’s services
- Partner requirements
- No SLA

If you require access to Google public infrastructure and cannot satisfy Google’s peering requirements, you can connect via a Carrier Peering partner. Work directly with your service provider to get the connection you need and to understand the partner’s requirements. For a full list of available service providers, see the links section of this video [https://cloud.google.com/interconnect/docs/how-to/carrier-peering#service_providers] .

Now, just like Direct Peering, Carrier Peering does not have an SLA.



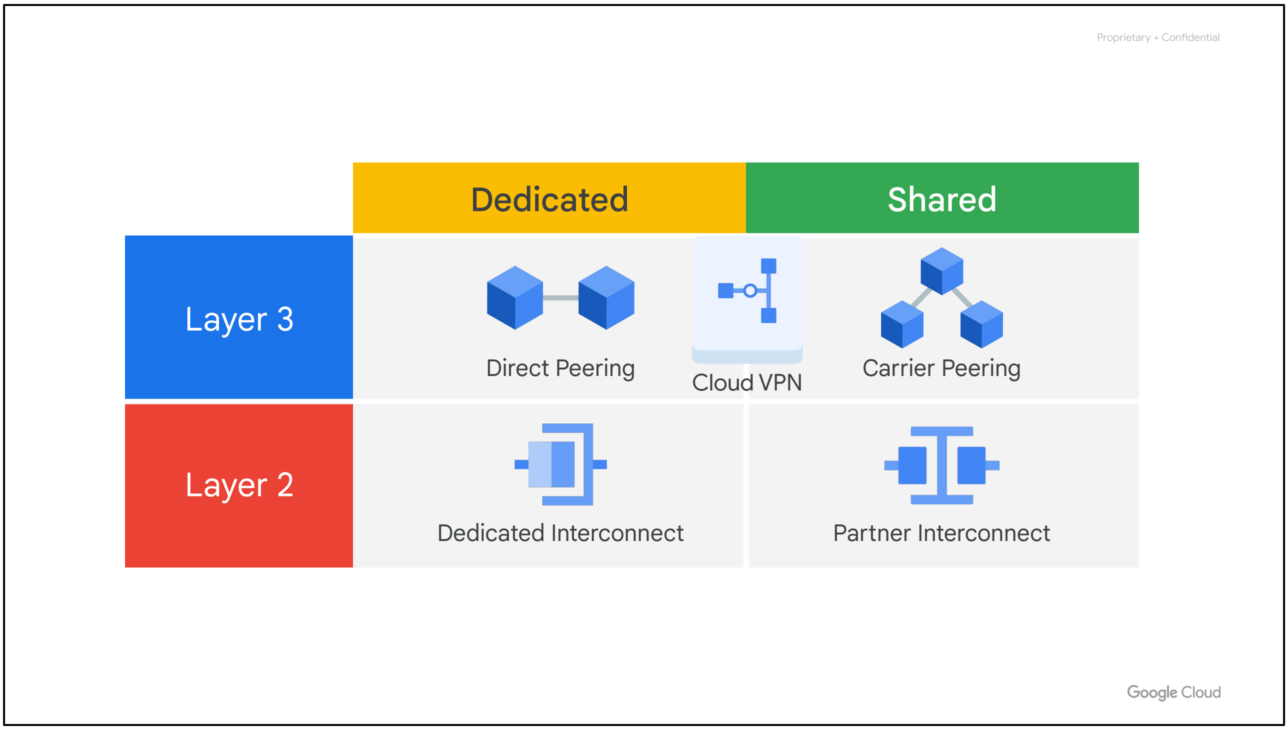
Comparison of Peering options

Connection	Provides	Capacity	Requirements	Access Type
Direct Peering	Dedicated, direct connection to Google's network	10 Gbps Per link	Connection in Google Cloud PoPs	Public IP addresses
Carrier Peering	Peering through service provider to Google's public network	Varies based on partner offering	Service provider	

Google Cloud

Let me compare the peering options that we just discussed. All of these options provide public IP address access to all of Google's services. The main differences are capacity and the requirements for using a service.

- Direct Peering has a capacity of 10 Gbps per link and requires you to have a connection in a GCP Edge Point of Presence.
- Carrier Peering's capacity and requirements vary depending on the service provider that you work with.

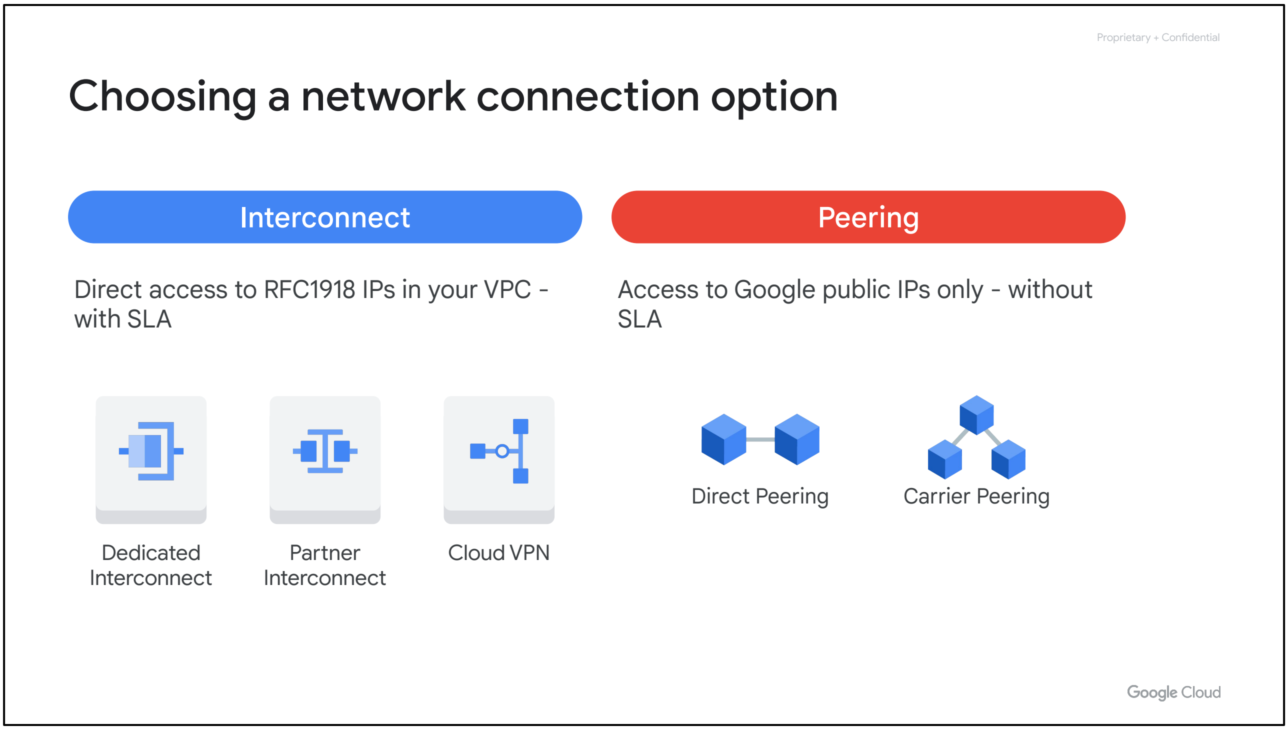


	Dedicated	Shared
Layer 3	Direct Peering	Carrier Peering
Layer 2	Dedicated Interconnect	Partner Interconnect

Cloud VPN

Now that we have discussed all the different connection services, let me help you determine which service best meets your hybrid connectivity needs.

I started this lesson by introducing the 5 different ways to connect your infrastructure to GCP. I split these services into Dedicated versus Shared connections and Layer 2 versus Layer 3 connections.



Choosing a network connection option

Interconnect

Direct access to RFC1918 IPs in your VPC - with SLA

Dedicated Interconnect
Partner Interconnect
Cloud VPN

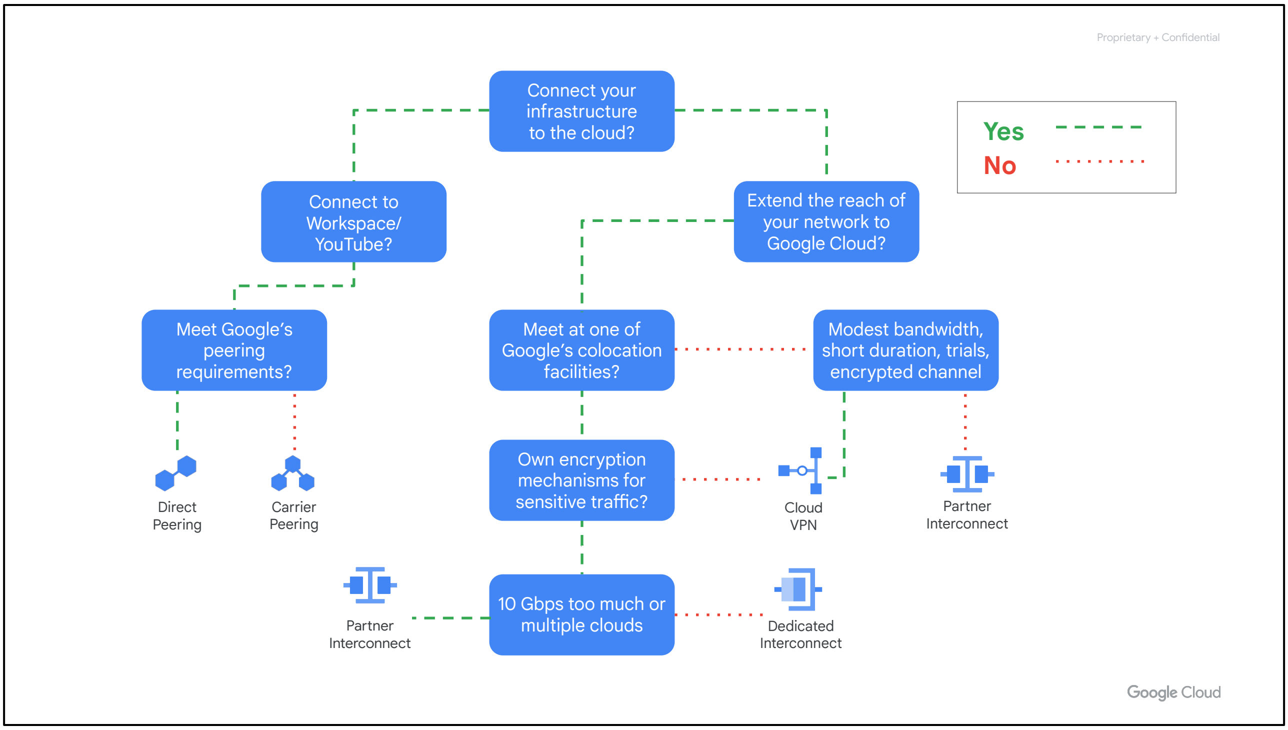
Peering

Access to Google public IPs only - without SLA

Direct Peering
Carrier Peering

Another way to organize these services is by Interconnect services and by Peering services.

Interconnect services provide direct access to RFC1918 IP addresses in your VPC, with an SLA. Peering services, in contrast, offer access to Google public IP addresses only, without an SLA.



Proprietary + Confidential

Yes - - - - -
No · · · · · · · ·

Connect your infrastructure to the cloud?

Connect to Workspace/ YouTube?

Extend the reach of your network to Google Cloud?

Meet Google's peering requirements?

Direct Peering

Carrier Peering

Meet at one of Google's colocation facilities?

Modest bandwidth, short duration, trials, encrypted channel

Own encryption mechanisms for sensitive traffic?

Cloud VPN

Partner Interconnect

10 Gbps too much or multiple clouds

Partner Interconnect

Dedicated Interconnect

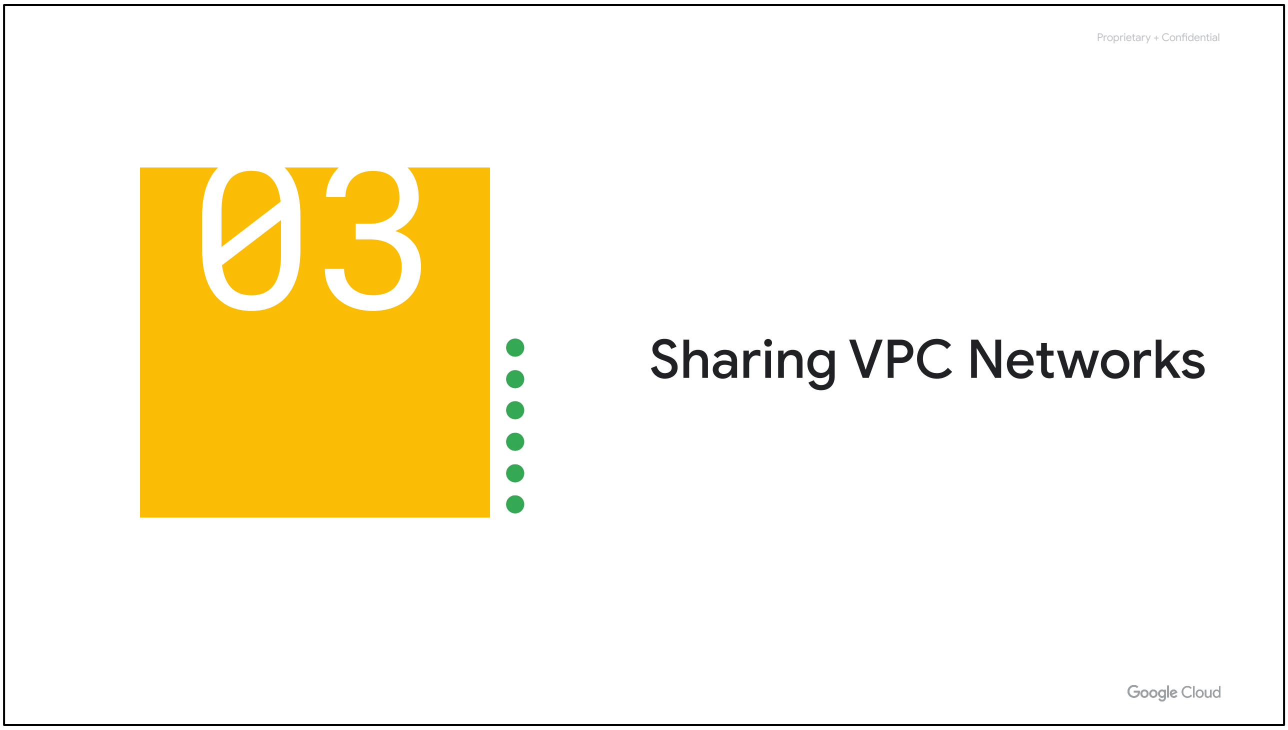
Google Cloud

Another way to choose the right service that meets your needs is with a flow diagram. Let me walk you through this diagram from the top, using the assumption that you want to extend your infrastructure to the cloud.

Ask yourself whether you need to extend your network for Workspace services, YouTube, or Google Cloud APIs. If you do, choose one of the Peering services. If you can meet Google's Direct Peering requirements, choose Direct Peering; otherwise, choose Carrier Peering.

If you don't need to extend your network for Workspace services or Google Cloud APIs but want to extend the reach of your network to Google Cloud, you want to pick one of the Interconnect services. If you cannot meet Google at one of its colocation facilities, choose Cloud VPN or Partner Interconnect. This choice will depend on your bandwidth and encryption requirements, along with the purpose of the connection. Specifically, if you have modest bandwidth needs, will use the connection for short durations and trials, and require an encrypted channel, choose Cloud VPN; otherwise, choose Partner Interconnect.

If you can meet Google at one of its colocation facilities, you might jump to Dedicated Interconnect; however, if you cannot provide your own encryption mechanisms for sensitive traffic, feel that a 10-Gbps connection is too big, or want access to multiple clouds, you'll want to consider Cloud VPN or Partner Interconnect instead.



03

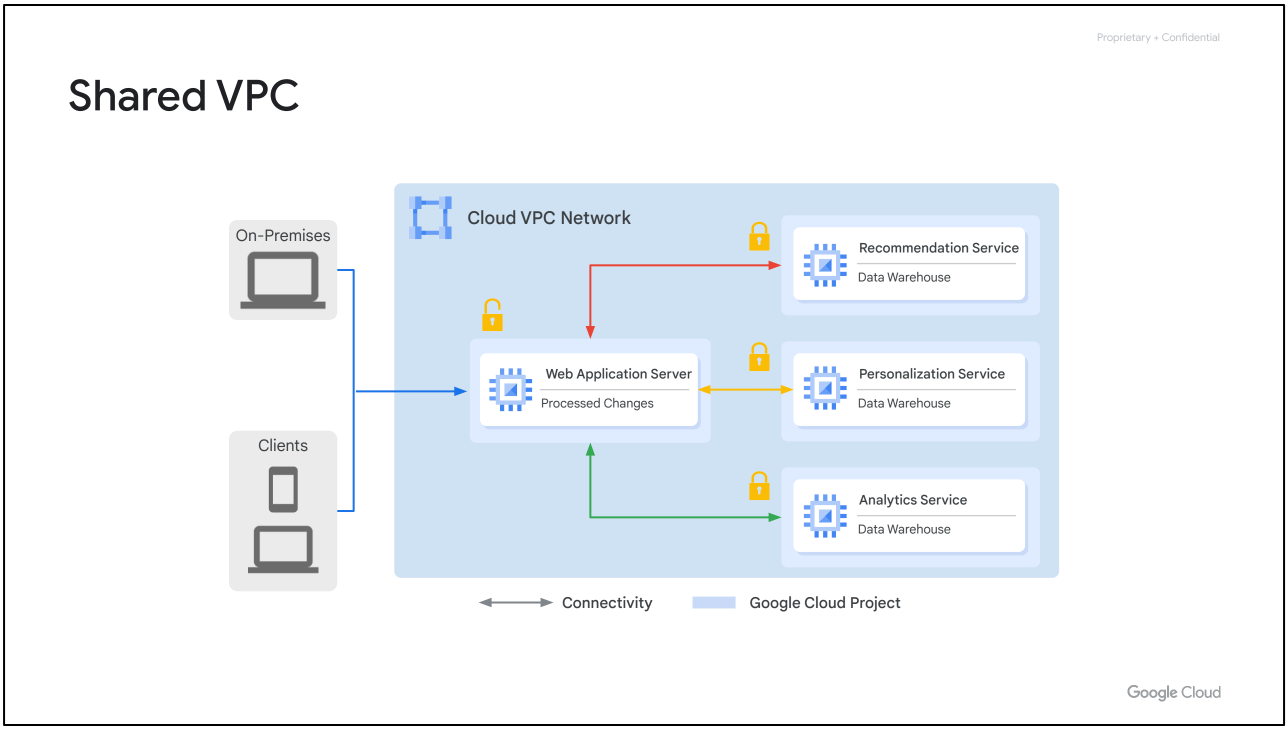
Sharing VPC Networks

Google Cloud

Let’s move our attention from hybrid connectivity to sharing VPC networks.

In the simplest cloud environment, a single project might have one VPC network, spanning many regions, with VM instances hosting very large and complicated applications. However, many organizations commonly deploy multiple, isolated projects with multiple VPC networks and subnets.

In this lesson, we are going to cover two configurations for sharing VPC networks across GCP projects. First, we will go over shared VPC, which allows you to share a network across several projects in your GCP organization. Then, we will go over VPC Network Peering, which allows you to configure private communication across projects in the same or different organizations.



Proprietary + Confidential

Shared VPC

On-Premises

Clients

Cloud VPC Network

Web Application Server
Processed Changes

Recommendation Service
Data Warehouse

Personalization Service
Data Warehouse

Analytics Service
Data Warehouse

⟷ Connectivity

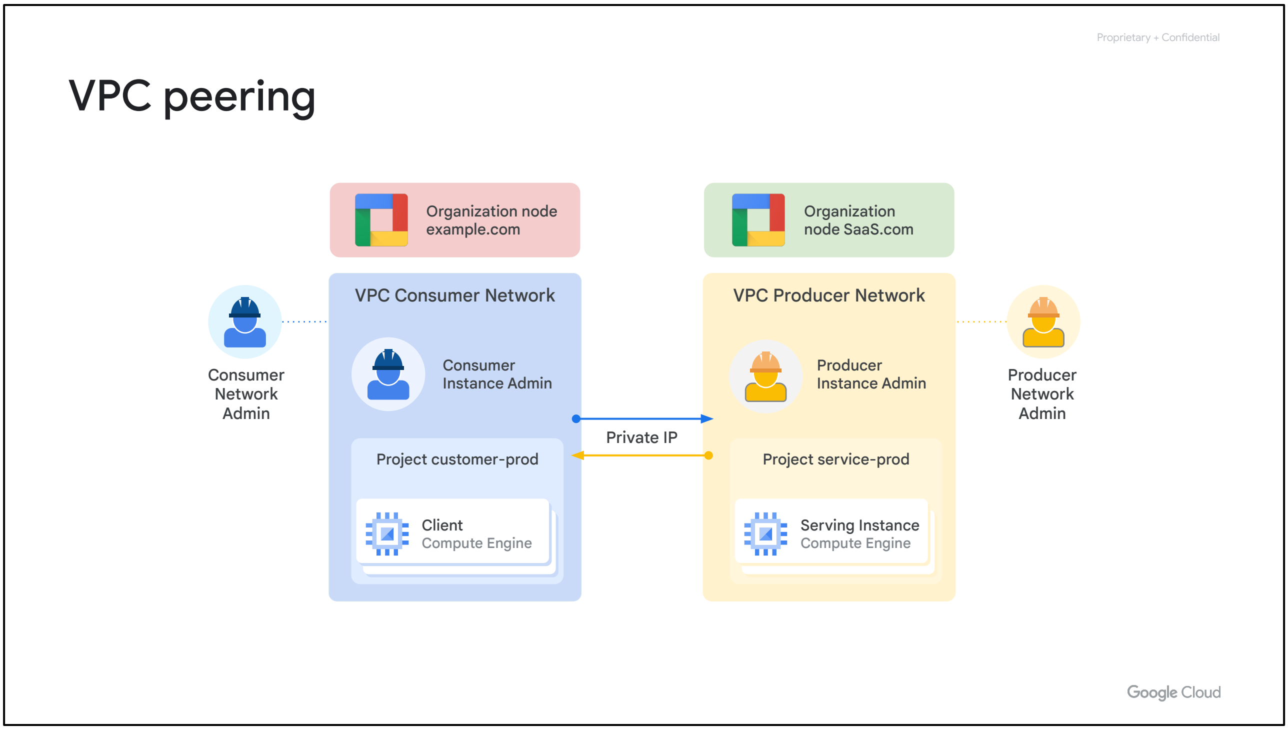
▨ Google Cloud Project

Google Cloud

Shared VPC allows an organization to connect resources from multiple projects to a common VPC network. This allows the resources to communicate with each other securely and efficiently using internal IPs from that network.

For example, in this diagram there is one network that belongs to the Web Application Server's project. This network is shared with three other projects, namely the Recommendation Service, the Personalization Service, and the Analytics Service. Each of those service projects has instances that are in the same network as the Web Application Server and allow for private communication to that server, using internal IP addresses. The Web Application Server communicates with clients and on-premises using the server's external IP address. The backend services, in contrast, cannot be reached externally because they only communicate using internal IP addresses.

When you use shared VPC, you designate a project as a host project and attach one or more other service projects to it. In this case, the Web Application Server's project is the host project, and the three other projects are the service projects. The overall VPC network is called the shared VPC network.



Proprietary + Confidential

VPC peering

Organization node example.com

Organization node SaaS.com

VPC Consumer Network

VPC Producer Network

Consumer Network Admin

Consumer Instance Admin

Producer Instance Admin

Producer Network Admin

Private IP

Project customer-prod

Project service-prod

Client Compute Engine

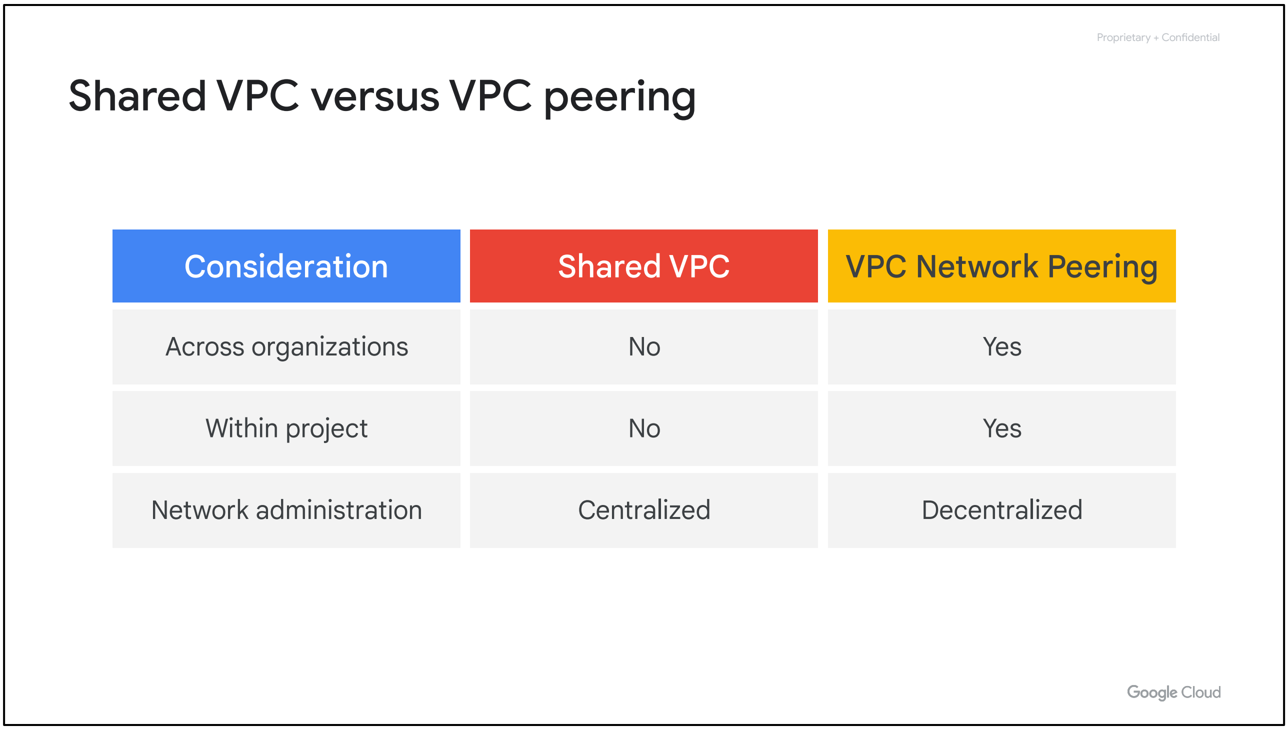
Serving Instance Compute Engine

Google Cloud

VPC Network Peering, in contrast, allows private RFC 1918 connectivity across two VPC networks, regardless of whether they belong to the same project or the same organization. Now, remember that each VPC network will have firewall rules that define what traffic is allowed or denied between the networks.

For example, in this diagram there are two organizations that represent a consumer and a producer, respectively. Each organization has its own organization node, VPC network, VM instances, Network Admin, and Instance Admin. In order for VPC Network Peering to be established successfully, the Producer Network Admin needs to peer the Producer Network with the Consumer Network, and the Consumer Network Admin needs to peer the Consumer Network with the Producer Network. When both peering connections are created, the VPC Network Peering session becomes Active and routes are exchanged. This allows the virtual machine instances to communicate privately using their internal IP addresses.

VPC Network Peering is a decentralized or distributed approach to multi-project networking, because each VPC network may remain under the control of separate administrator groups and maintains its own global firewall and routing tables. Historically, such projects would consider external IP addresses or VPNs to facilitate private communication between VPC networks. However, VPC Network Peering does not incur the network latency, security, and cost drawbacks that are present when using external IP addresses or VPNs.



Proprietary + Confidential

Shared VPC versus VPC peering

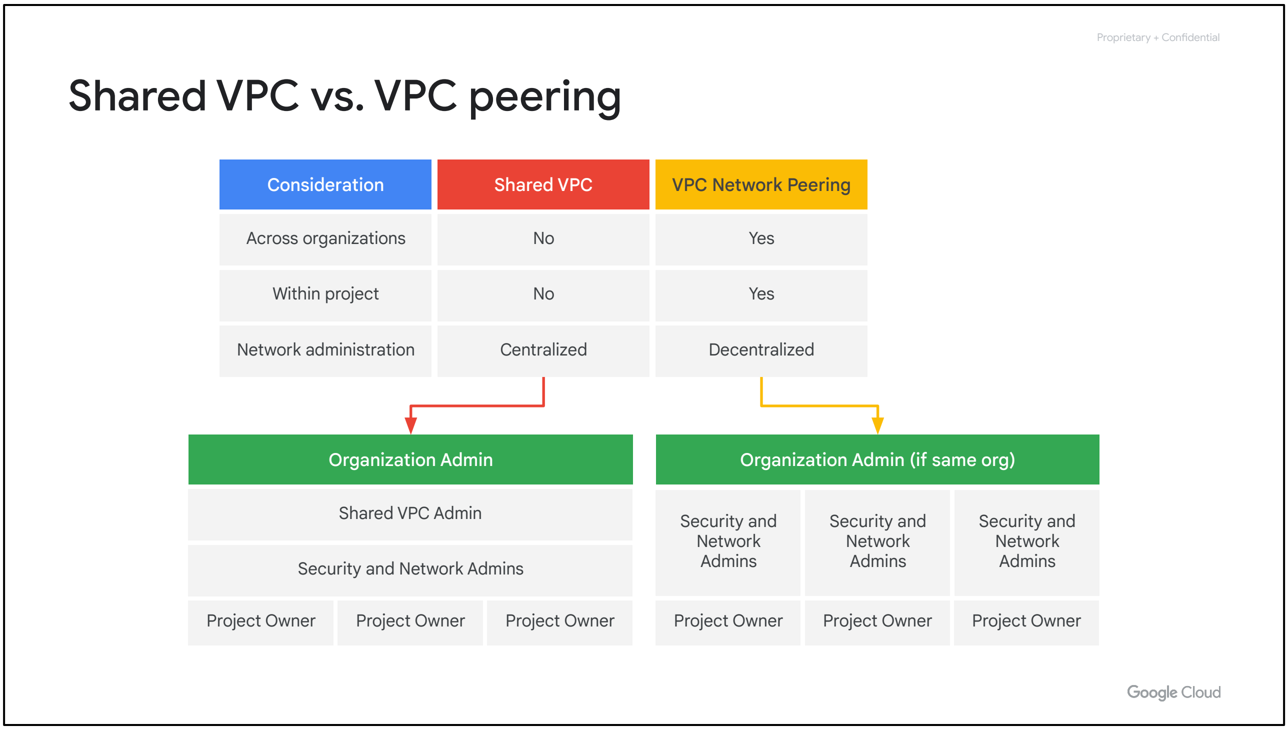
Consideration	Shared VPC	VPC Network Peering
Across organizations	No	Yes
Within project	No	Yes
Network administration	Centralized	Decentralized

Google Cloud

Now that we've talked about Shared VPC and VPC Network Peering, let me compare both of these configurations to help you decide which is appropriate for a given situation.

If you want to configure private communication between VPC networks in different organizations, you have to use VPC Network Peering. Shared VPC only works within the same organization.

Somewhat similarly, if you want to configure private communication between VPC networks in the same project, you have to use VPC Network Peering. This doesn't mean that the networks need to be in the same project, but they can be. Shared VPC only works across projects.



Proprietary + Confidential

Shared VPC vs. VPC peering

Consideration	Shared VPC	VPC Network Peering
Across organizations	No	Yes
Within project	No	Yes
Network administration	Centralized	Decentralized

Organization Admin

Shared VPC Admin

Security and Network Admins

Project Owner | Project Owner | Project Owner

Organization Admin (if same org)

Security and Network Admins | Security and Network Admins | Security and Network Admins

Project Owner | Project Owner | Project Owner

Google Cloud

In my opinion, the biggest difference between the two configurations is the network administration models. Shared VPC is a centralized approach to multi-project networking, because security and network policy occurs in a single designated VPC network. In contrast, VPC Network Peering is a decentralized approach, because each VPC network can remain under the control of separate administrator groups and maintains its own global firewall and routing tables.