Cloud Computing #4

Cloud Networking

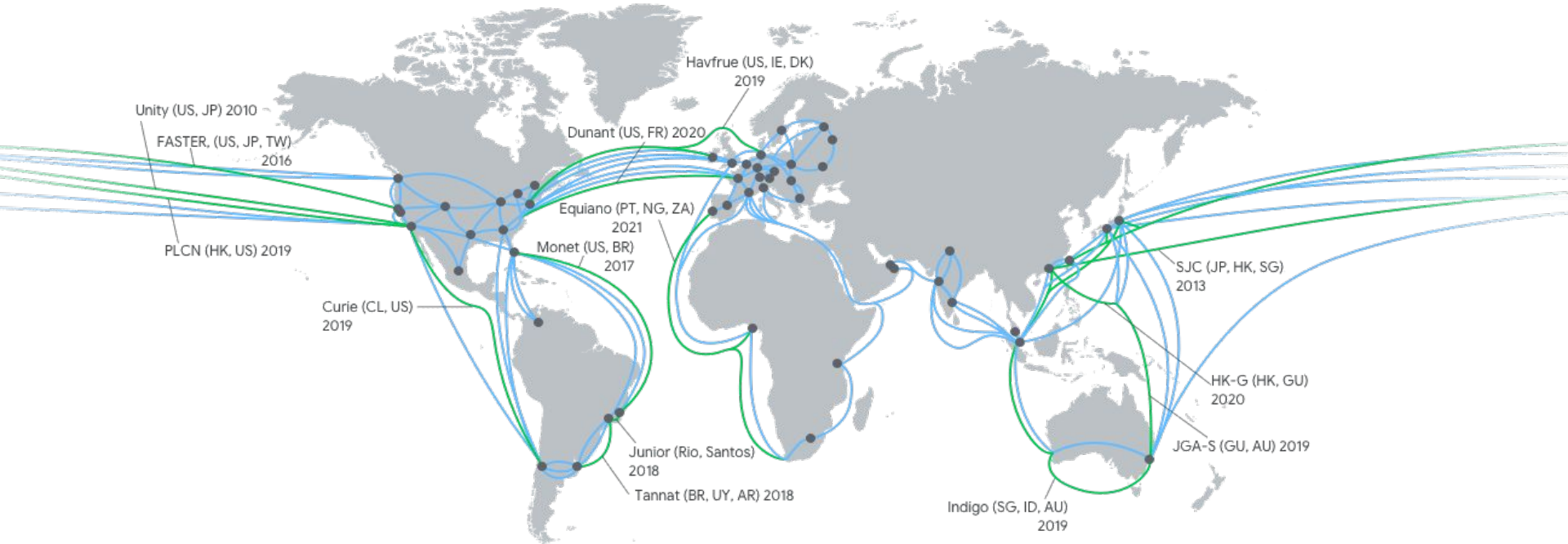
Topics

1. VPC networks
2. DNS topology
3. Connectivity options
4. Reference architectures
5. Load balancing
6. Network access control

VPC networks

Google's global network infrastructure

Hundreds of thousands of miles of fiber optic cable connecting all of our data center regions and 100+ points of presence.



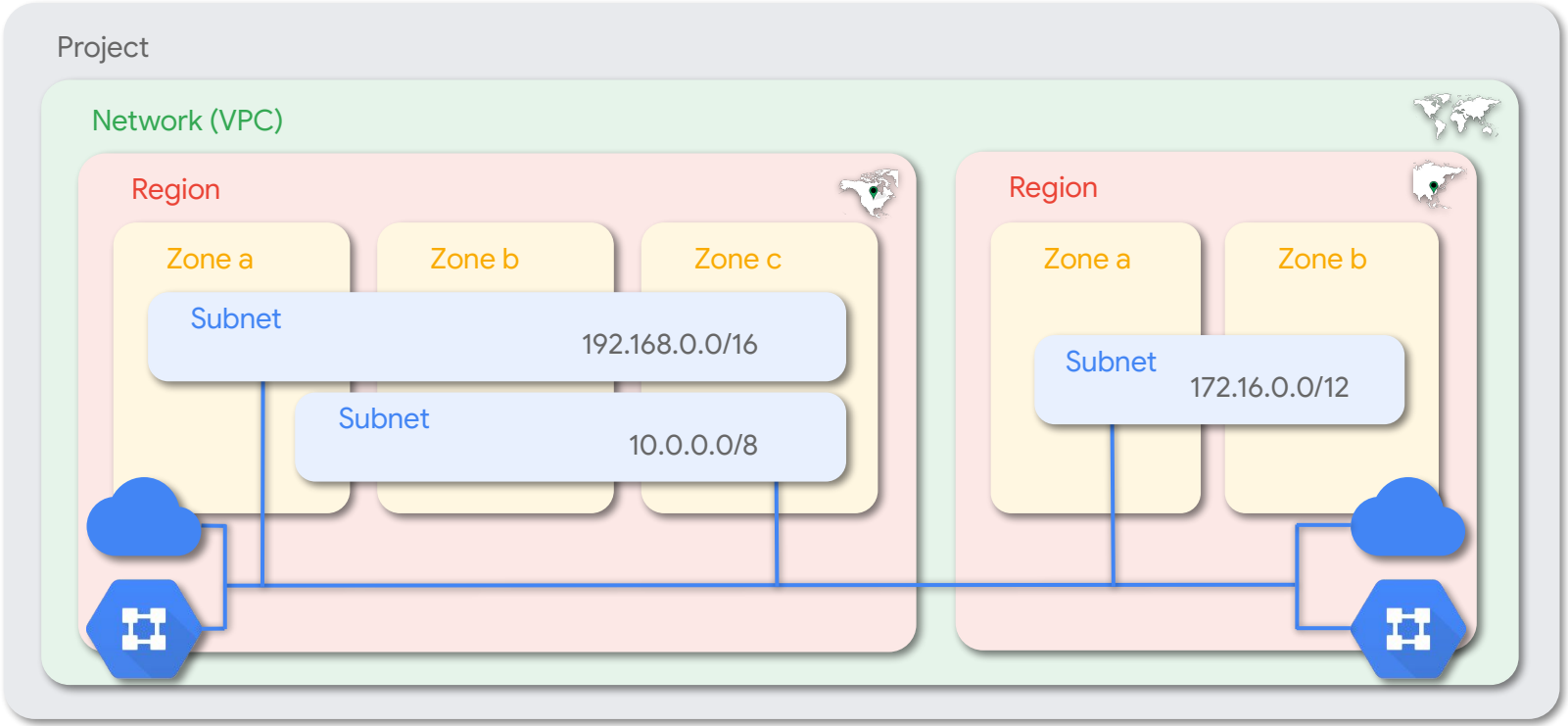
Network tiers

Premium

Standard

https://peering.google.com/#/infrastructure

Network concepts

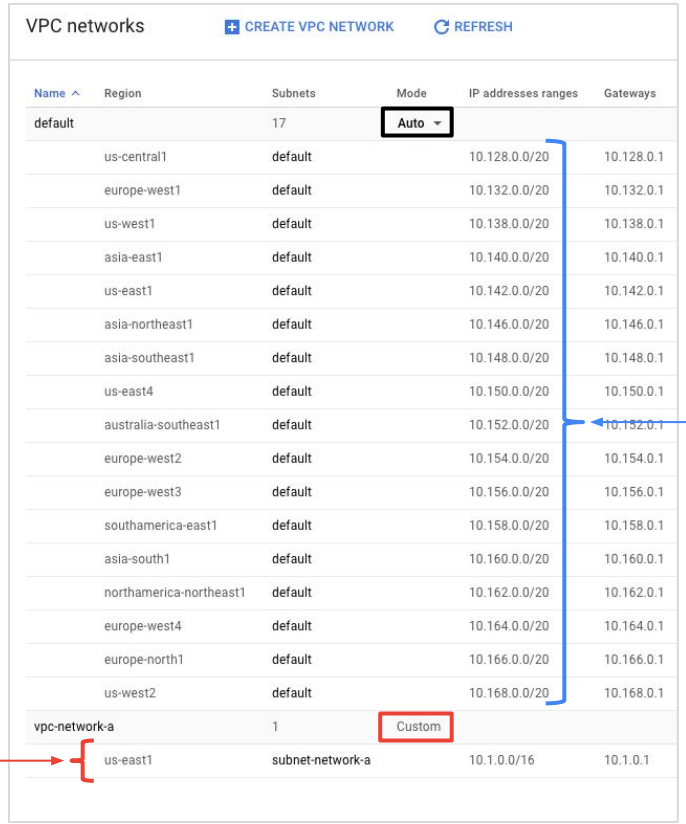


Subnet creation modes

Best Practice

Custom subnet mode

- Network admin **defines subnets and IP ranges**
- No default firewalls rules
- **Expandable** to any RFC-1918 size
- Good for
  - **Production** environments
  - **Preventing CIDR overlap** between environments

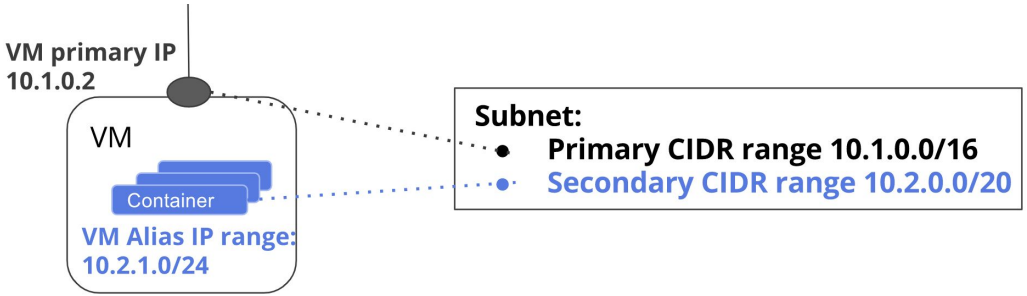


Auto subnet mode

- Default network **when project is created**
- **Default /20** subnetwork per region
- **Expandable** up to /16
- Subnets created as new regions are launched
- Comes with **default FW rules** (e.g. TCP 22)
- Good for isolated use cases (PoCs, testing)

Subnet CIDR ranges

	Primary	Secondary
Configuration	Mandatory - one per subnet	Optional - multiple ranges are supported
Used for	Allocation of VM primary IP Reserved IP's	Allocating a different IP to multiple microservices running in a VM (e.g., containers, GKE pods).
Extendable	Range can be extended, but not shrinked	No



IP addressing

VM instances

Internal IP

- Allocated from subnet primary range
- Ephemeral (default) or static
- Multi-NIC support

External IP

- Ephemeral or reserved

Load Balancers

Forwarding rules are required for load balancers

External/internal IP is required depending on the load balancer type

VPC Routes

- VPC level management
- Applies to all the endpoints in a VPC network.
- Selectively apply routes to a subnet of VM instances based on network tags
- Internet access is enabled by a route, which is automatically created

Route	Type	Created by	Next Hop	Restrictions	Exchanged with VPC Peering
Subnet route	System	System	VPC network	Cannot be removed	Automatic
Static route	Custom	User	Instance IP/name Cloud VPN	Must be broader than a subnet IP range	Flag controlled
Dynamic route	Custom	Cloud router (BGP session)	BGP peer	Must be broader than a subnet IP range	Flag controlled

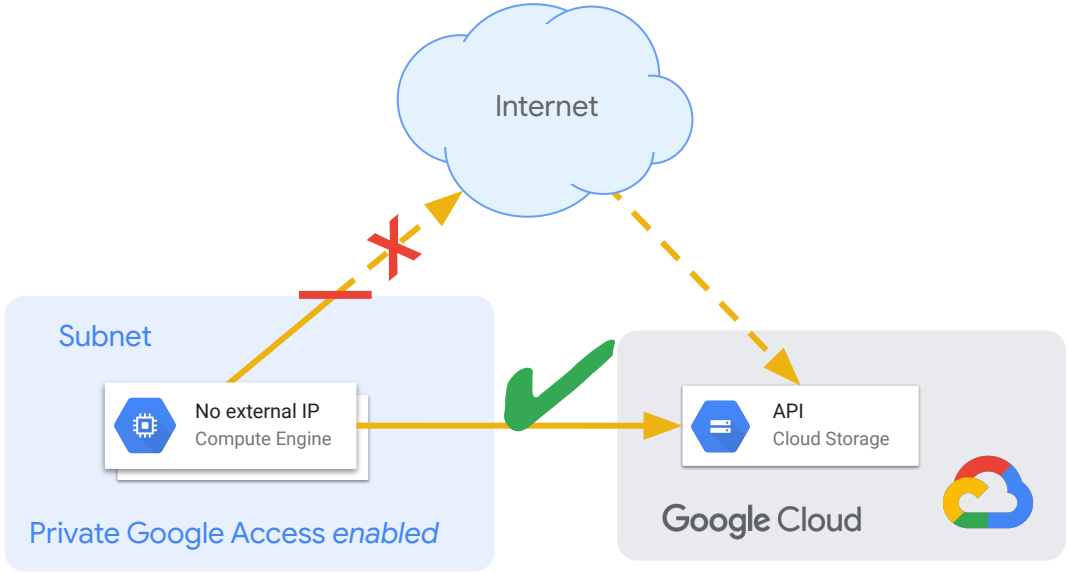
Private Google access

Compute instances require public IP addresses to communicate directly with resources outside of their network.

Problem:
Instances without public IP addresses can't access Google Cloud's public API endpoints.

Solution:
Enable **Private Google Access** in the subnetwork the instance is attached to.

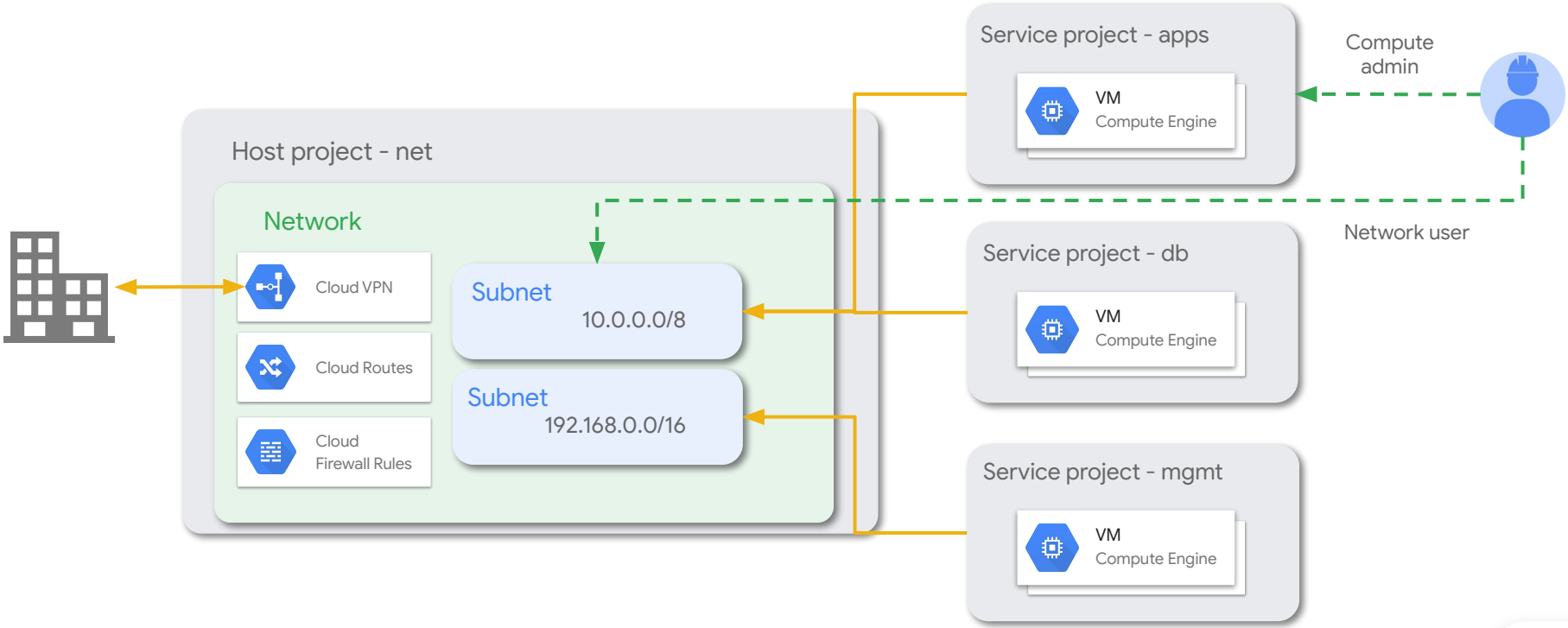
Can be stretched to on-premise through Cloud VPN or Cloud Interconnect



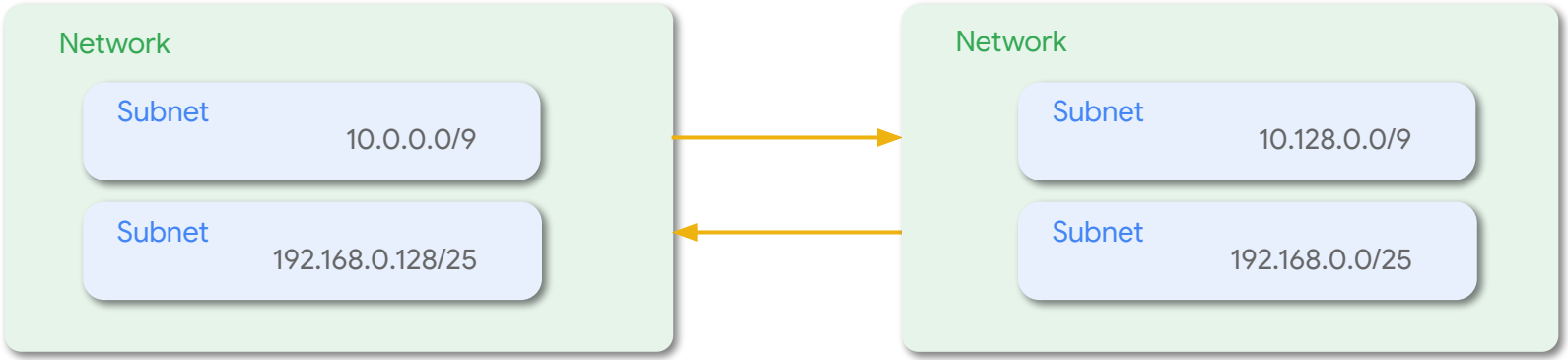
Cross project communication

	Shared VPC	VPC Peering	Cloud VPN
Network services management (Firewalls, subnets, routes, VPN, DNS)	Central management of shared network resources	Clear network and security administrative boundaries	Clear network and security administrative boundaries
Transitivity	N/A	Non-transitive	Transitive
Scale	1000 service projects or more, depending on multiple factors	Up to 25 peered networks	Approximately 100 connected projects
Pricing	General network pricing	General network pricing	General network pricing. Excluding intra-zone traffic which is billed as interzone.
Performance implication	None	None	Throughput limited based on number of tunnels (1.5 to 3 Gbps per tunnel)

Shared VPC networks

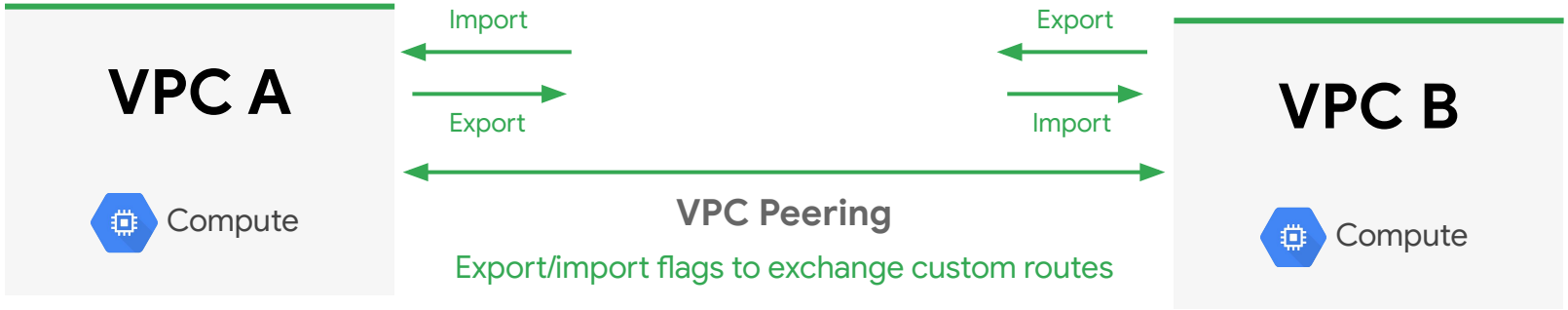


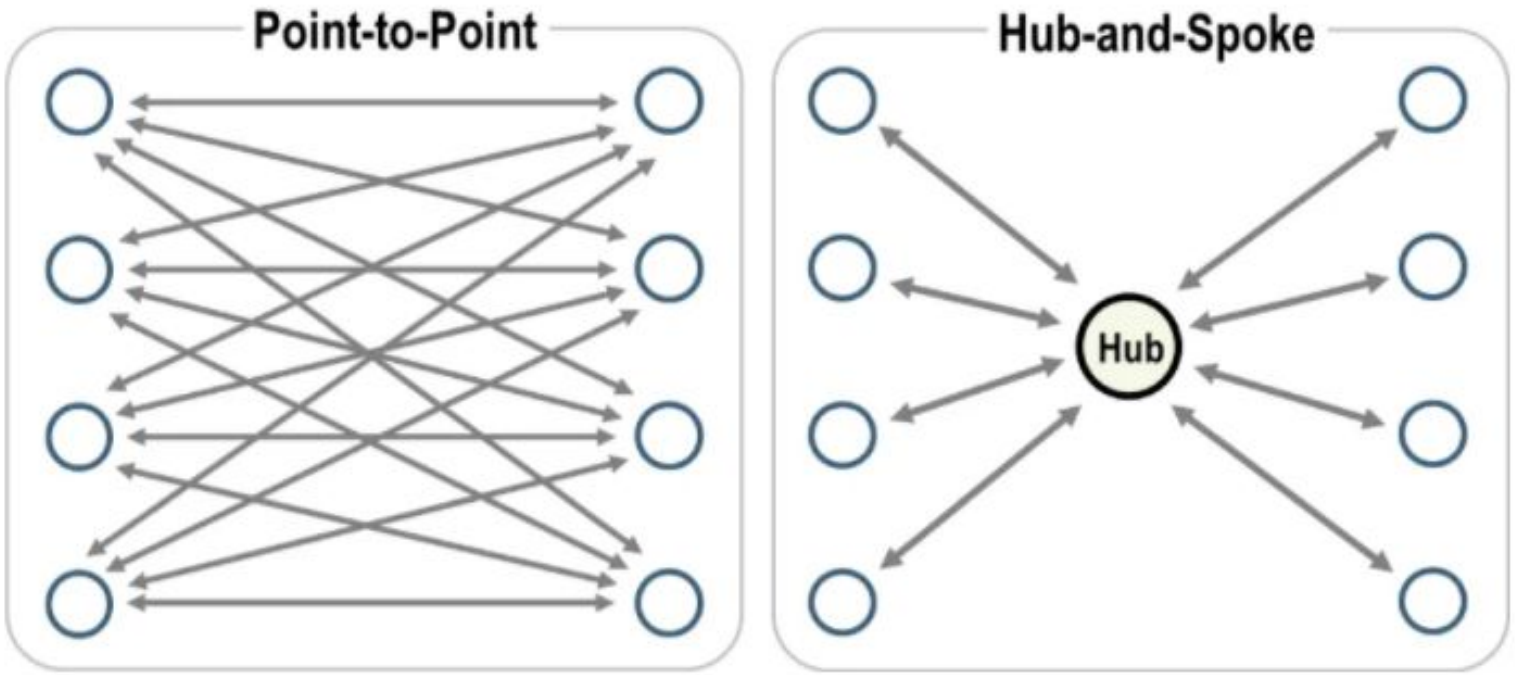
VPC network peering



Exchanging custom routes

Route	Type	Exchange with VPC Peering
Subnet route	System	Automatic
Static route	Custom	Flag controlled
Dynamic route	Custom	Flag controlled



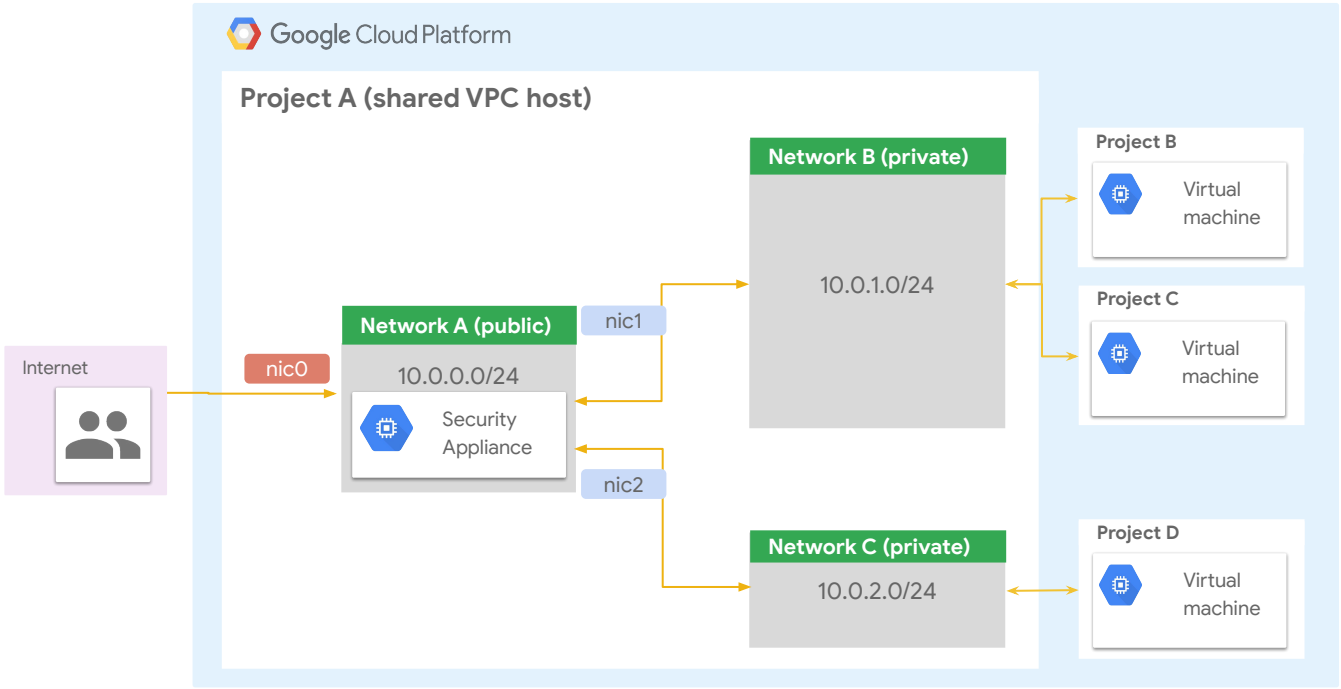


Point-to-Point and Hub-and-Spoke Networks

Connecting network and security appliances

Multiple NIC Architecture

- IDS/IPS: North-South and East-West
  - VPC to VPC only
- Application firewall
- WAN optimization
- Up to 8 NICs
- Up to 16 GB (2 GB per vCPU)



VPC network best practices

Custom mode VPCs	Prevent overlapping IPs and control subnet creation by creating VPCs with custom subnet creation mode.
Use Shared VPC	Reduce management and topology complexity by making use of Shared VPC where fit.
Fewer subnets	Group similar applications into fewer, more manageable and larger subnets.
Restrict network configuration	Apply organization policies to 1) skip creation of default network for new projects, 2) restrict shared VPC host projects and subnets, and 3) restrict VPC peering usage.
Consider quota limitations	Ensure the design scales to your needs by considering limitations on each network component.

Key decisions

1. How will cloud resources communicate with each other?
2. How will resources be segmented into networks and subnets?
3. What are the scalability requirements concerning networking components?
4. How will name resolution be solved among cloud resources, and between the cloud and connected environments?
5. What strategies will be used to connect GCP with corporate networks?
6. How will cloud resources communicate with the internet?

LAB 1

VPC Networking Fundamentals

1 hour 5 Credits

https://www.qwiklabs.com/focuses/1229?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=15442501

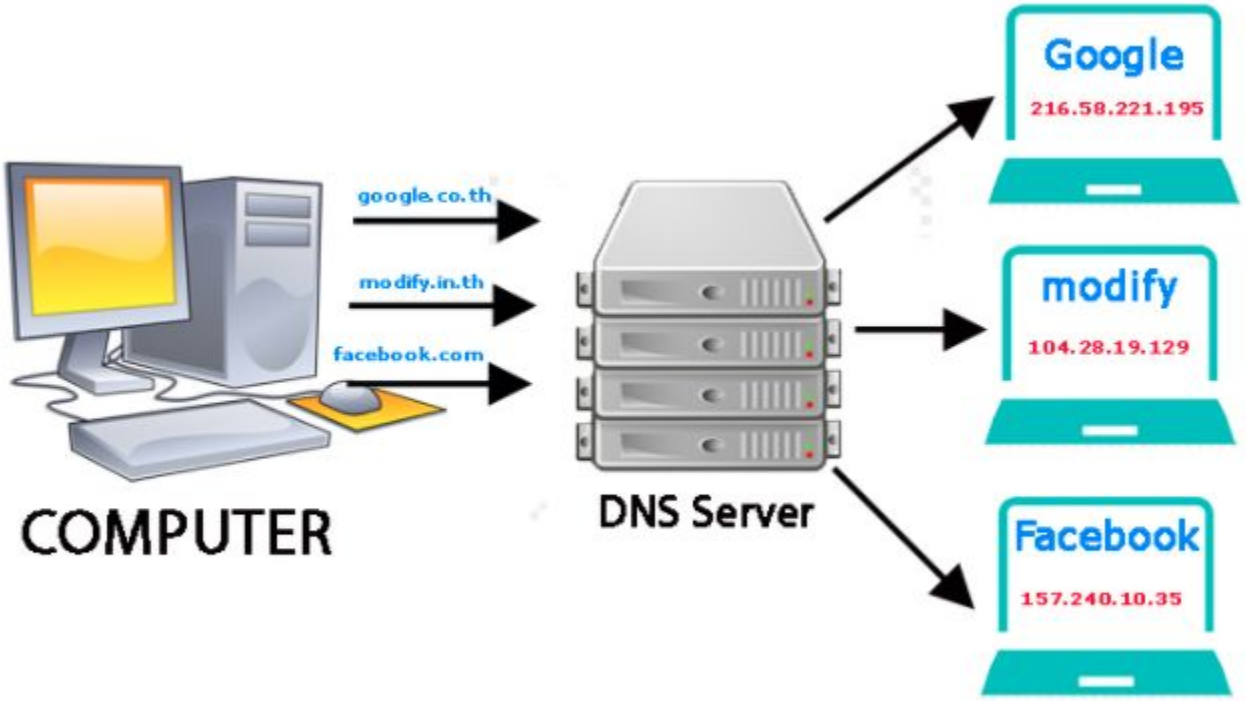
GSP210

Google Cloud Self-Paced Labs

Break

10 นาที

DNS topology



Google Cloud

DNS ของ TOP

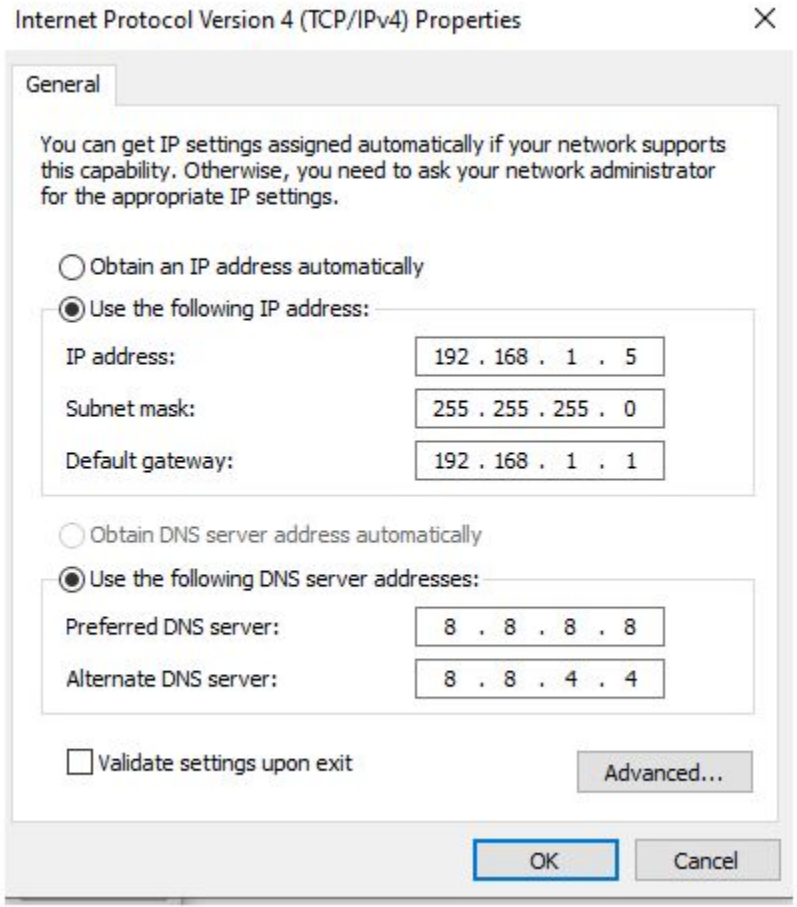
- 203.113.144.66
- 203.113.111.11

DNS ของ Google

- 8.8.8.8
- 8.8.4.4

DNS ของ Cloudflare

- 1.1.1.1



Google Cloud

DNS options

An internal metadata server acts as DNS resolver, and is automatically set as such as part of DHCP leases

Internal DNS

Records are automatically created for VMs primary and internal IP's with the following FQDN:

- [INSTANCE_NAME].[ZONE].c.[PROJECT_ID].internal

Used for resolution within the same project and VPC

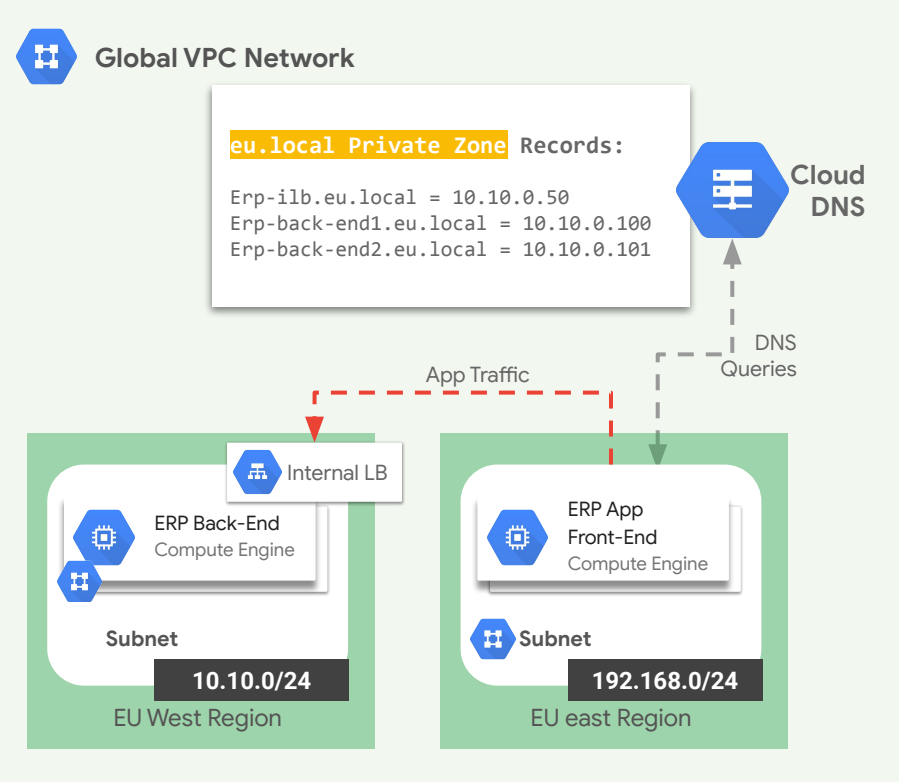
Cloud DNS

Scalable, reliable (**100% SLA**), and managed authoritative DNS service for public and private records offering

Private: Used for providing a namespace that is only visible inside the VPC

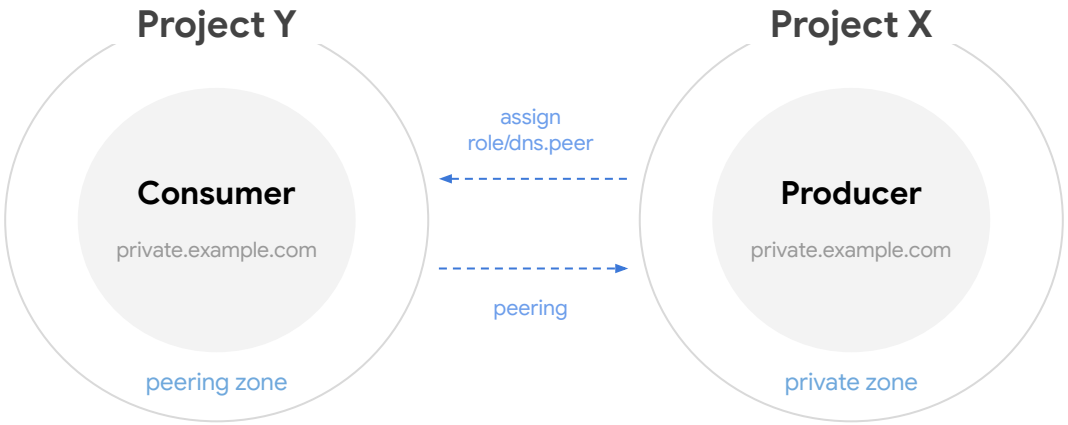
Public: Used for providing authoritative DNS resolution to clients on the public internet.

Cloud DNS: Private DNS zones



- Internal facing DNS records (e.g., VMs, LBs)
- Requests must be submitted through the metadata server
- Can only be queried by authorized VPC networks in the same project, unless DNS peering is configured

Cloud DNS: DNS peering (Beta)



What

- DNS Peering allows DNS queries to be sent from one zone's namespace to another VPC
- Does not require connectivity between the VPC's
- One way only
- Recursion depth of 2

Use cases

- DNS peering alongside DNS forwarding resembles a hub-and-spoke networking model, and alleviates the issue with multiple forwarding zones to the same on-premises environment
- SaaS providers

Cloud DNS: DNS forwarding

Outbound policy

Use for: Alternative name servers, when all DNS traffic needs to be monitored

Specify a list of alternative name servers to use for all DNS queries

Inbound policy

Use for: On-premises to GCP

Allows querying VPC network name resolution services through inbound forwarders.

Available to systems connected with Cloud VPN and Cloud Interconnect

Forwarding zone

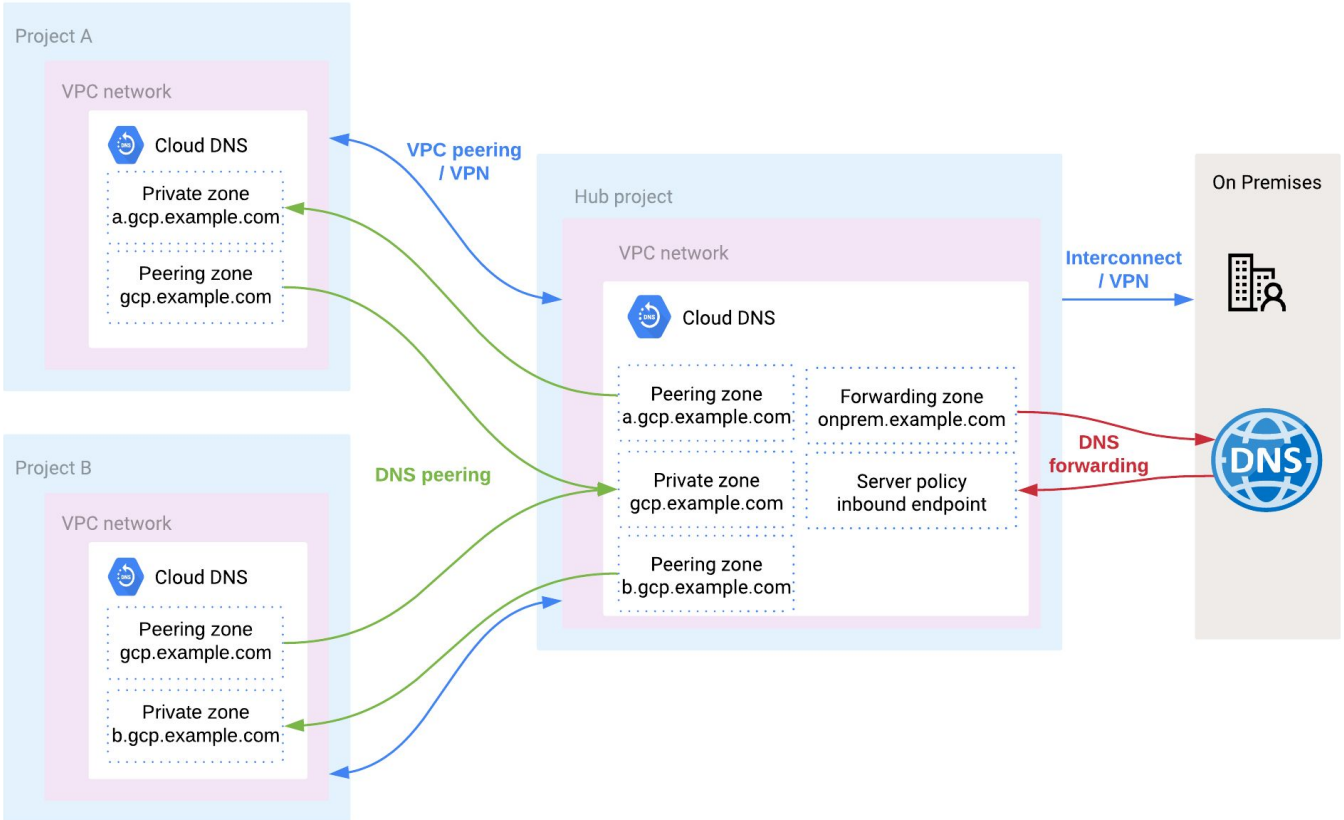
Use for: GCP to on-premises

All queries matching a forwarding zone are are forwarded to a set of destination name servers

Queries have the same IP range as source (35.199.192.0/19 block).

Cannot be set between GCP projects

Cloud DNS: Hub-and-spoke model



Key decisions

1. How will cloud resources communicate with each other?
2. How will resources be segmented into networks and subnets?
3. What are the scalability requirements concerning networking components?
4. How will name resolution be solved among cloud resources, and between the cloud and connected environments?
5. What strategies will be used to connect GCP with corporate networks?
6. How will cloud resources communicate with the internet?

Connectivity options

Connectivity options

Public Internet (IPSEC VPN)

- Fastest way to connect to the cloud or between clouds
- Leverages existing internet network connectivity
- Supports high availability and aggregated bandwidth with **1.5 to 3 Gbps per tunnel**
- Static/dynamic (BGP) based VPN

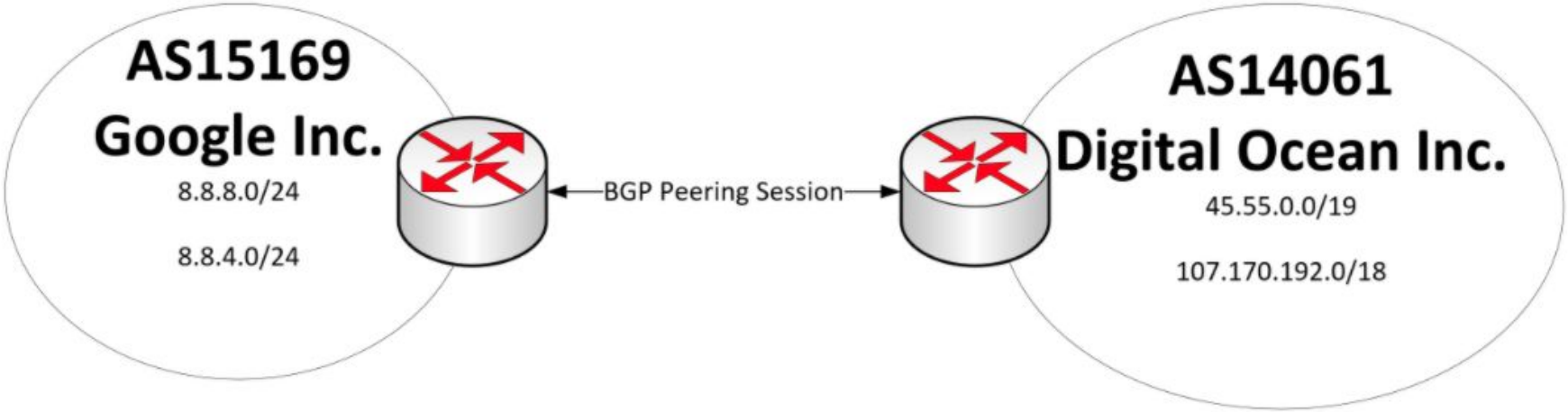
Cloud Interconnect

- Enterprise-grade, private connectivity to GCP
- Provisioned as a dedicated link to a Google PoP or via a partner
- Dedicated Interconnect: Highest bandwidth with **10 Gbps and 100 Gbps links**
- Partner Interconnect offers more flexible subscriptions (**50 Mbps to 10 Gbps**)

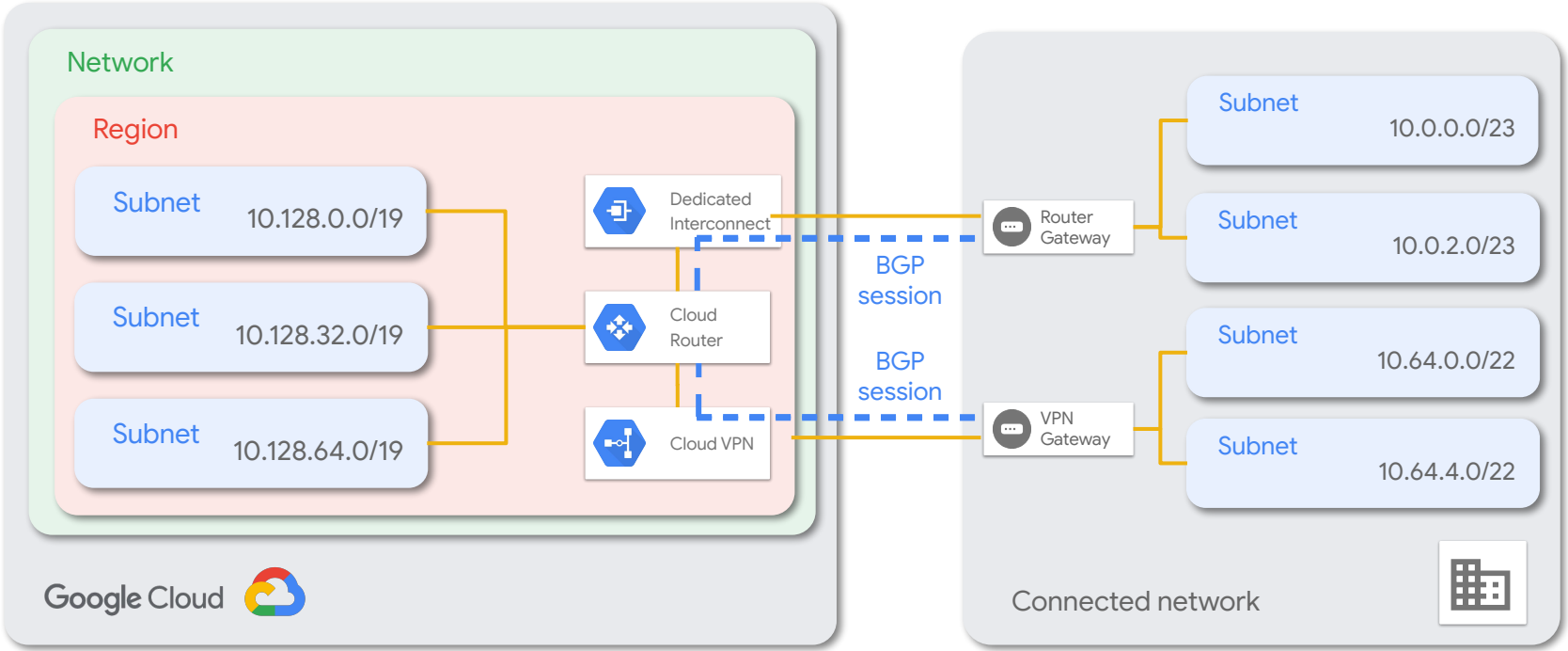
Peering

- Access G Suite and Google services, as well as GCP with reduced egress rates
- Utilizes existing BGP route selection and internet routing
- Greater control of peering facilities
- Direct or carrier

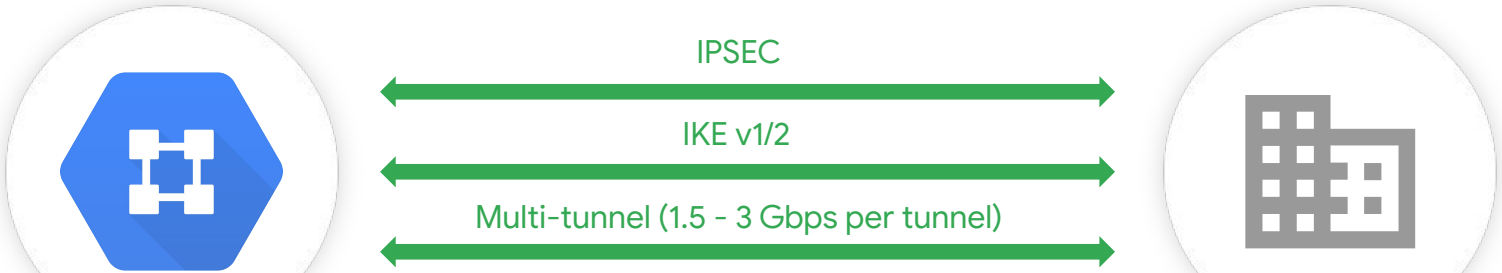
BGP Peering Session



Cloud router



Cloud VPN



Static, public IP required

Google recommends reserving
RFC 1918 IP space to avoid overlap

Static, public IP required

Classic vs HA VPN

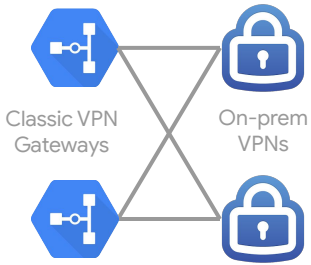
Classic VPN

Routing options:

- Dynamic (BGP)
- Static (route- or policy-based)

Manual HA setup:

- Gateways have a **single interface and external IP**



HA VPN

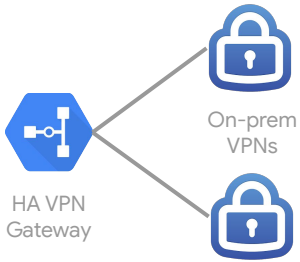
Common pattern

Dynamic routing only

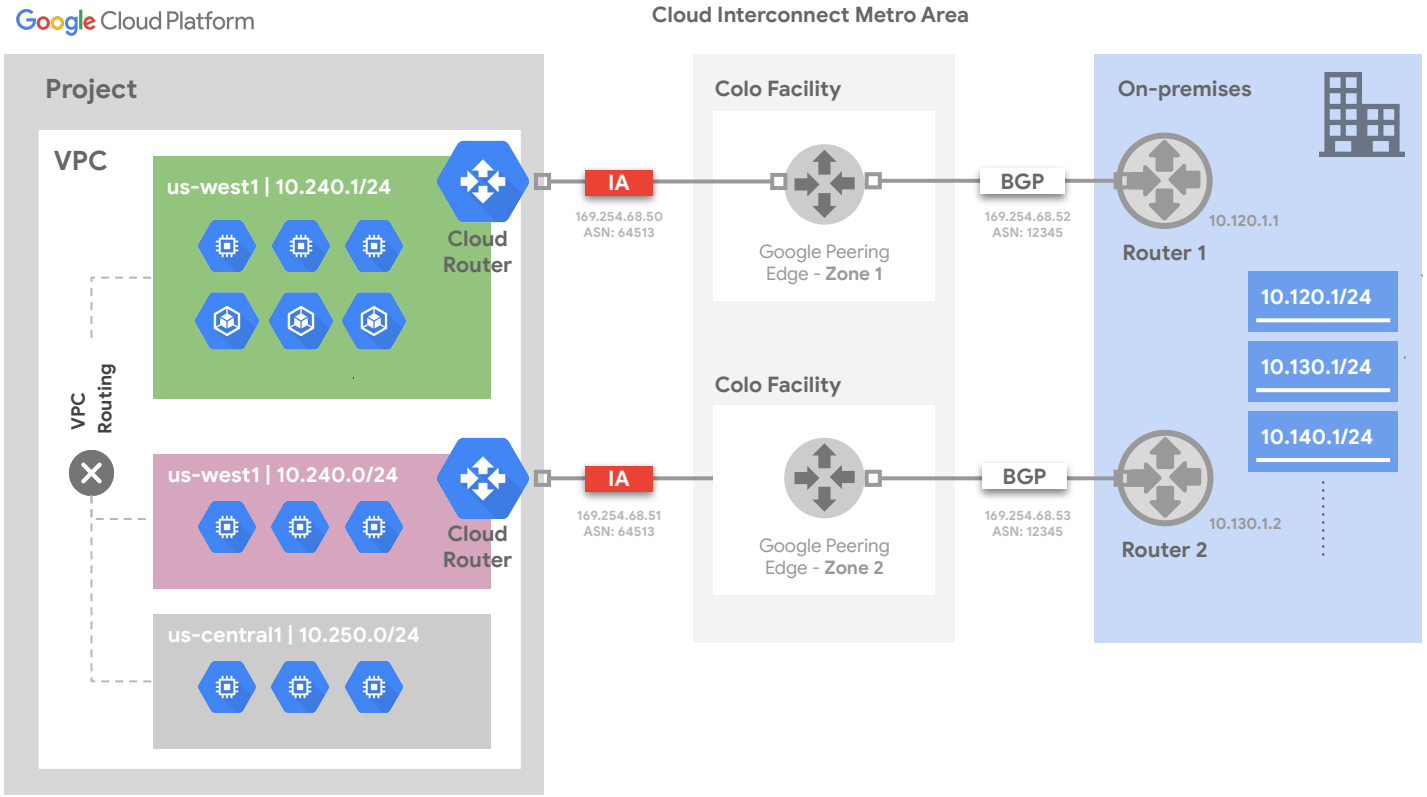
Easy HA setup:

- Gateways have **two totally separate interfaces** (physically and logically)
- **99.99% SLA**

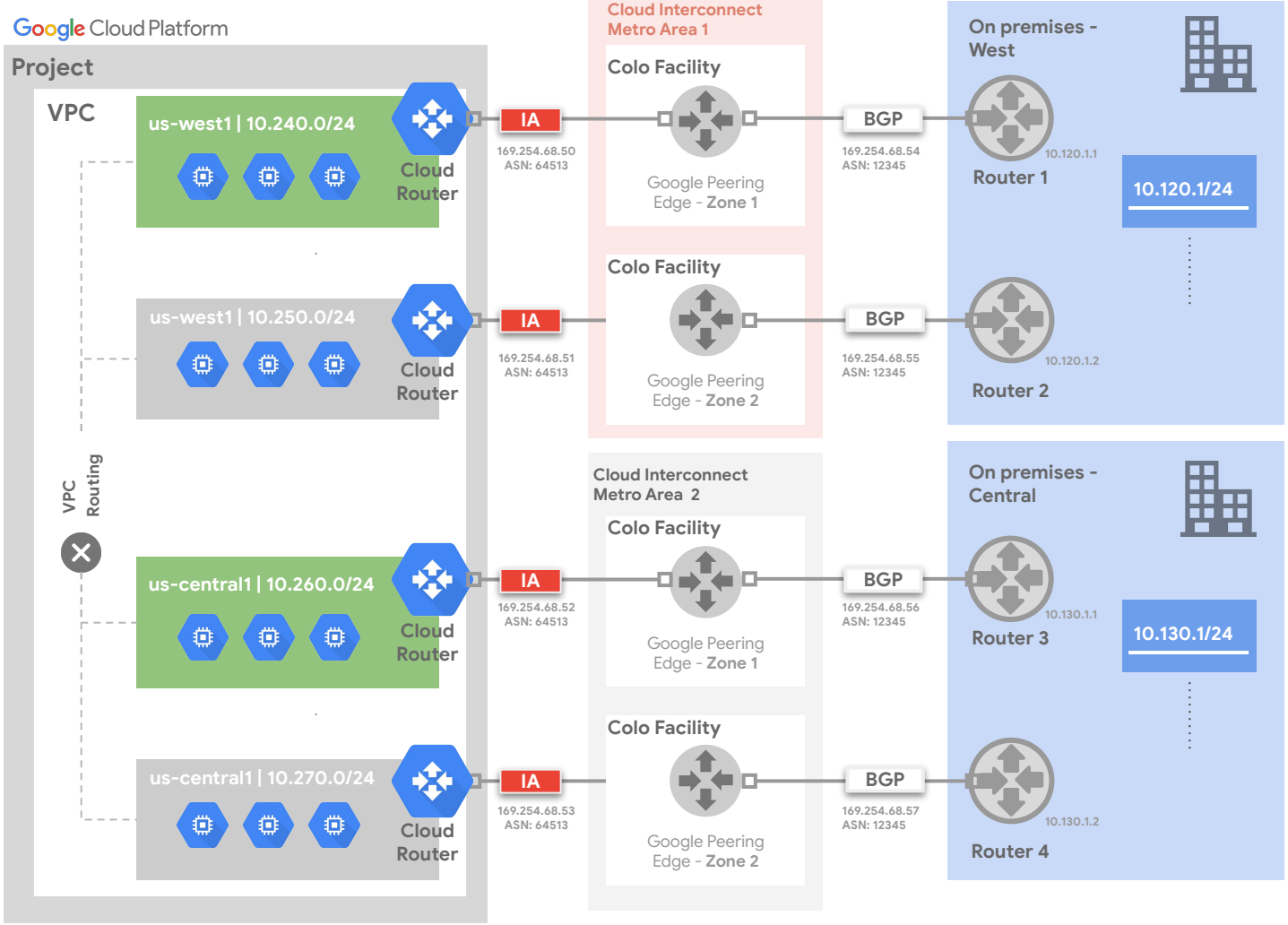
Recommended choice for new deployments



Dedicated Interconnect



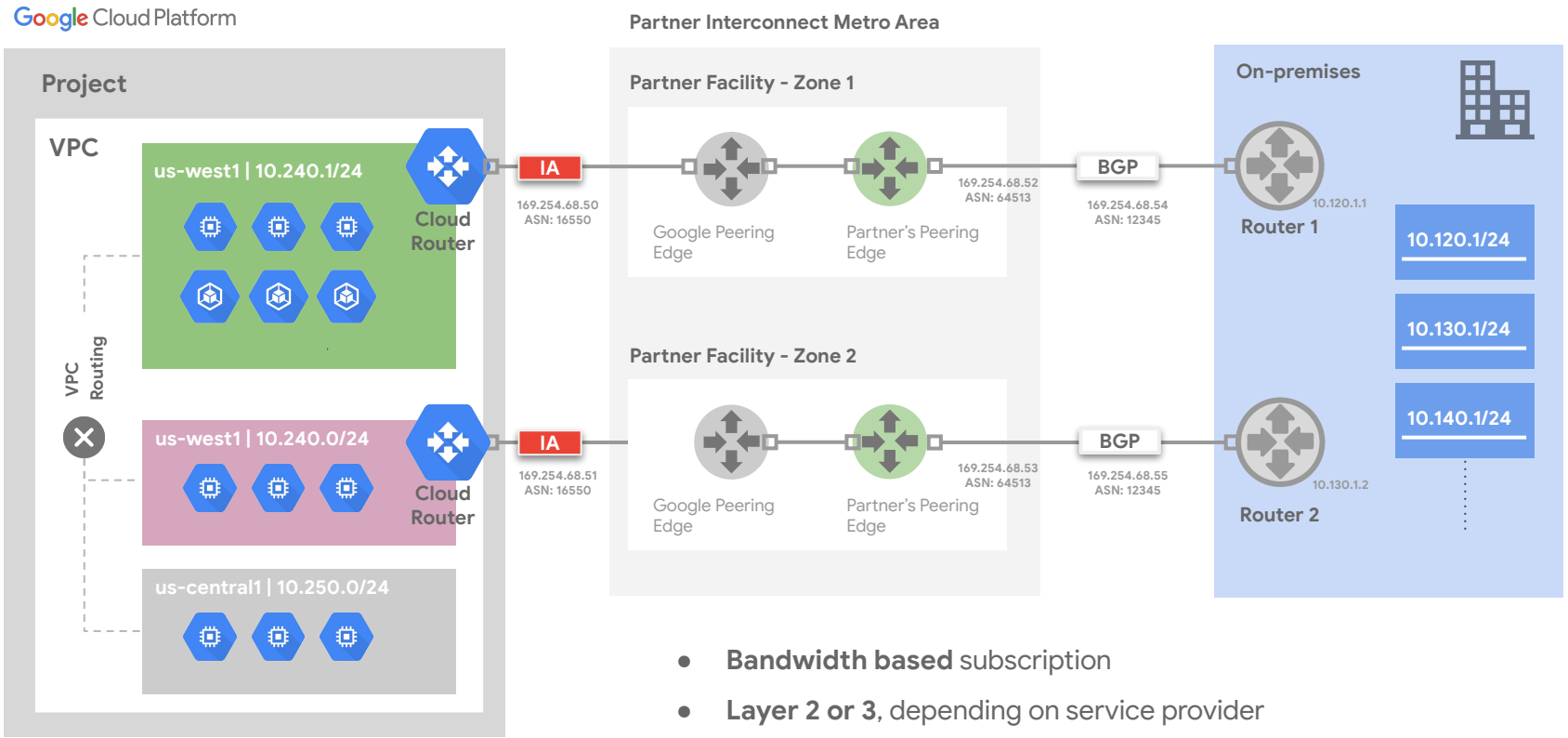
- **Layer 2** connectivity
- Up to **eight 10 Gbps** links, or **two 100 Gbps** links
- Same Interconnect can link to **multiple VPCs** within the same project
- 99.9% or 99.99% SLAs depending on the architecture chosen



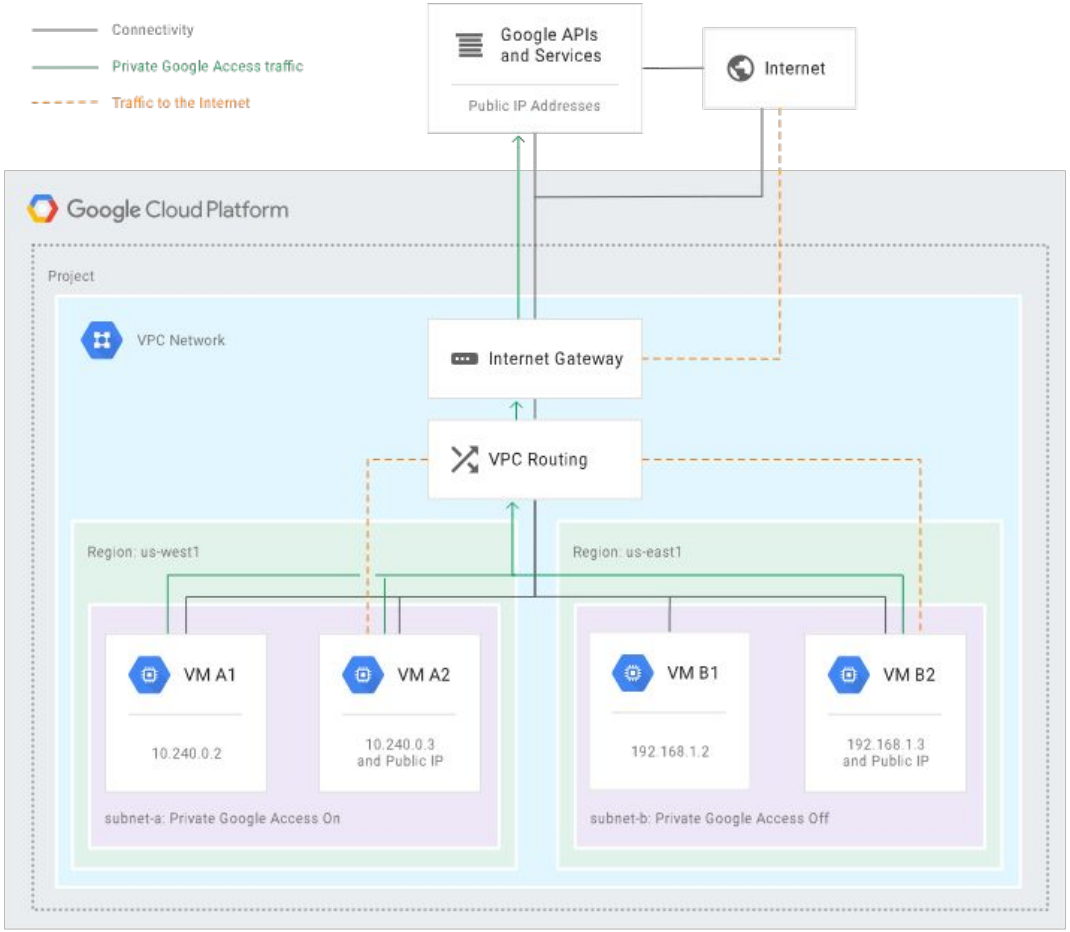
Dedicated Interconnect 99.99% SLA config

Best practice

Partner Interconnect



- **Bandwidth based** subscription
- **Layer 2 or 3**, depending on service provider
- 99.9% or 99.99% SLAs

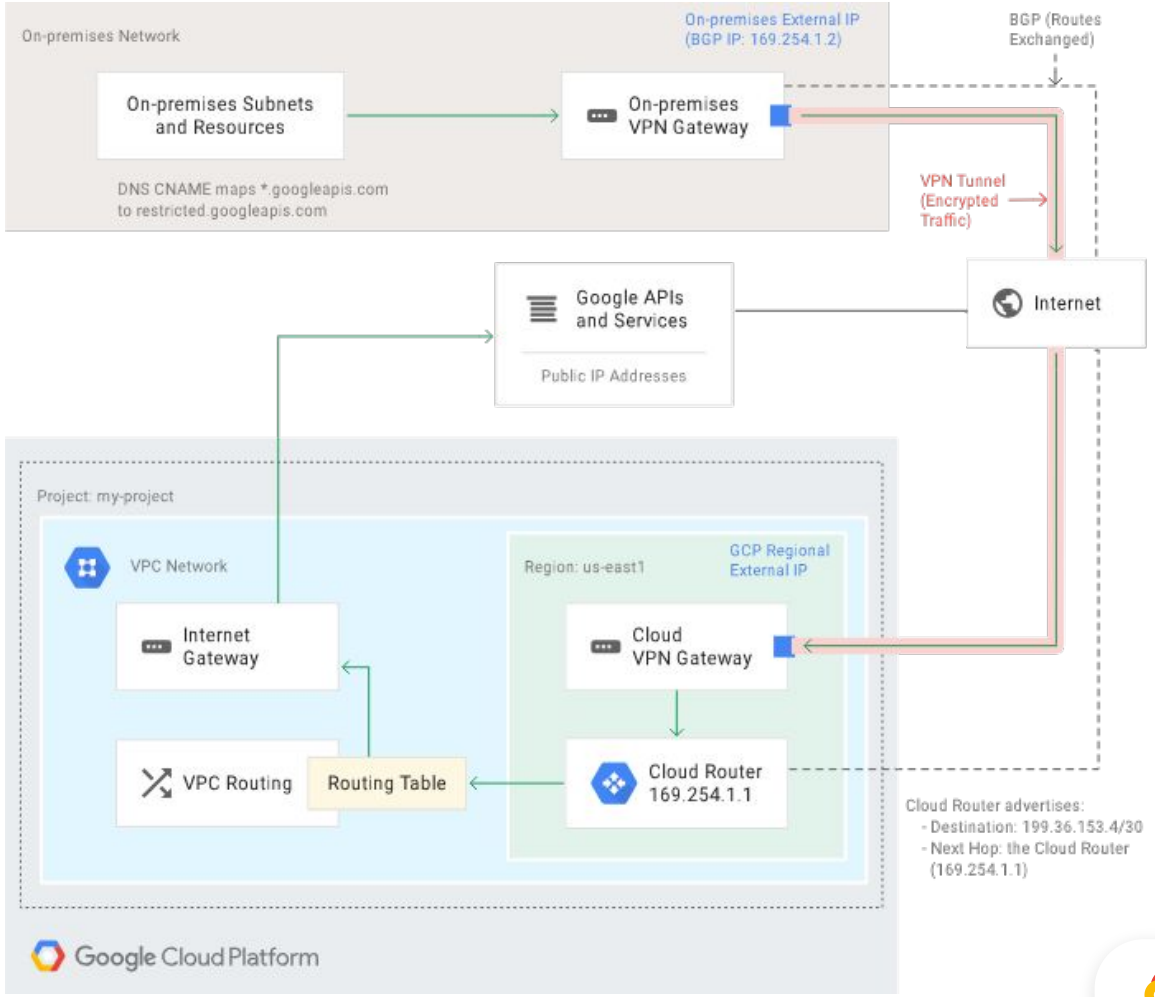


Private Google Access

If your instances will access Google APIs, enable private access. This access is disabled by default.

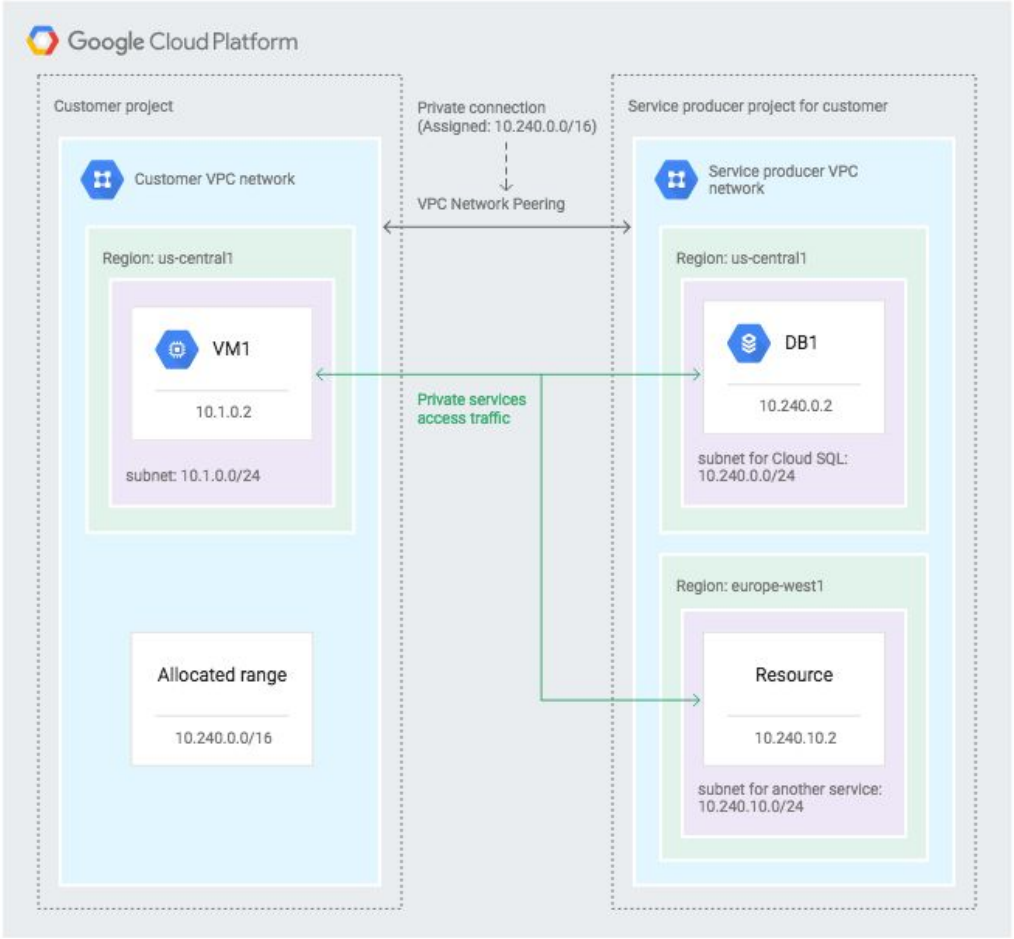
Private Google Access for on-premises hosts (Beta)

On-premises hosts can reach Google APIs and services over a Cloud VPN or Cloud Interconnect connection from your data center to GCP.



Private Services Access

Connect to specific Google and third-party services without assigning external IP addresses to your GCP and Google or third-party resources.



Key decisions

1. How will cloud resources communicate with each other?
2. How will resources be segmented into networks and subnets?
3. What are the scalability requirements concerning networking components?
4. How will name resolution be solved among cloud resources, and between the cloud and connected environments?
5. What strategies will be used to connect GCP with corporate networks?
6. How will cloud resources communicate with the internet?

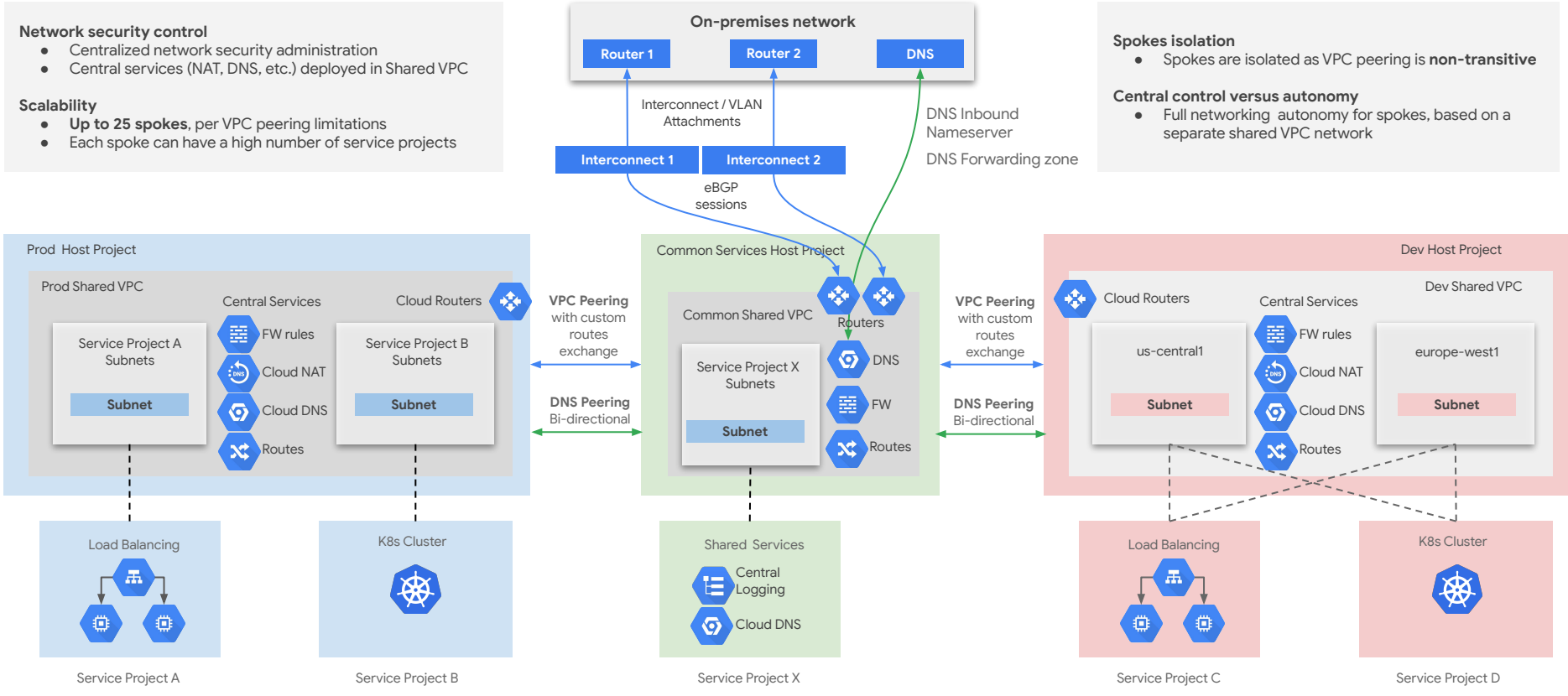
Reference architectures

Reference architecture

Hub-and-spoke with VPC peering - Segmentation based on environments

Network security control
- Centralized network security administration
- Central services (NAT, DNS, etc.) deployed in Shared VPC

Scalability
- **Up to 25 spokes**, per VPC peering limitations
- Each spoke can have a high number of service projects



Spokes isolation
- Spokes are isolated as VPC peering is **non-transitive**

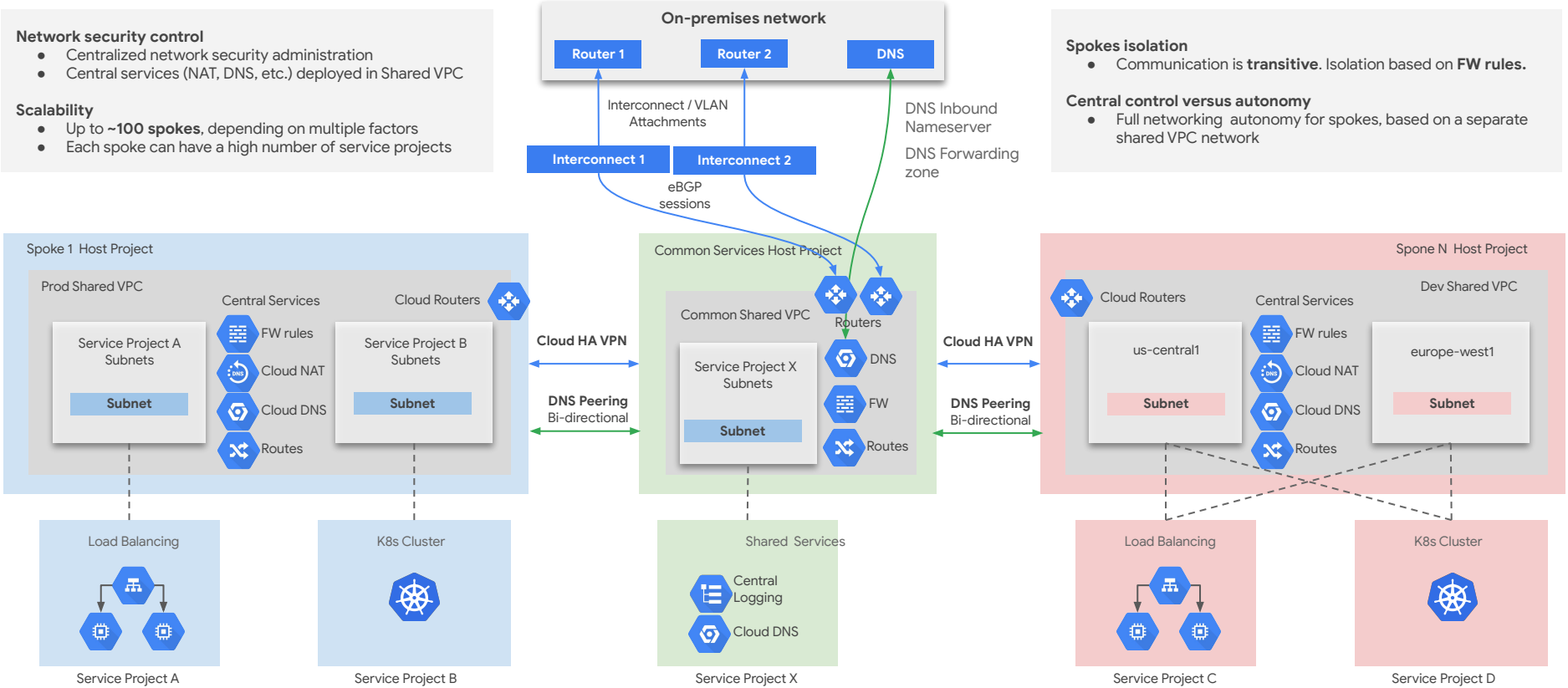
Central control versus autonomy
- Full networking autonomy for spokes, based on a separate shared VPC network

Reference architecture

Hub-and-spoke with Cloud VPN - Multi-tenancy

Network security control
- Centralized network security administration
- Central services (NAT, DNS, etc.) deployed in Shared VPC

Scalability
- Up to **~100 spokes**, depending on multiple factors
- Each spoke can have a high number of service projects



Spokes isolation
- Communication is **transitive**. Isolation based on **FW rules.**

Central control versus autonomy
- Full networking autonomy for spokes, based on a separate shared VPC network

Load balancing

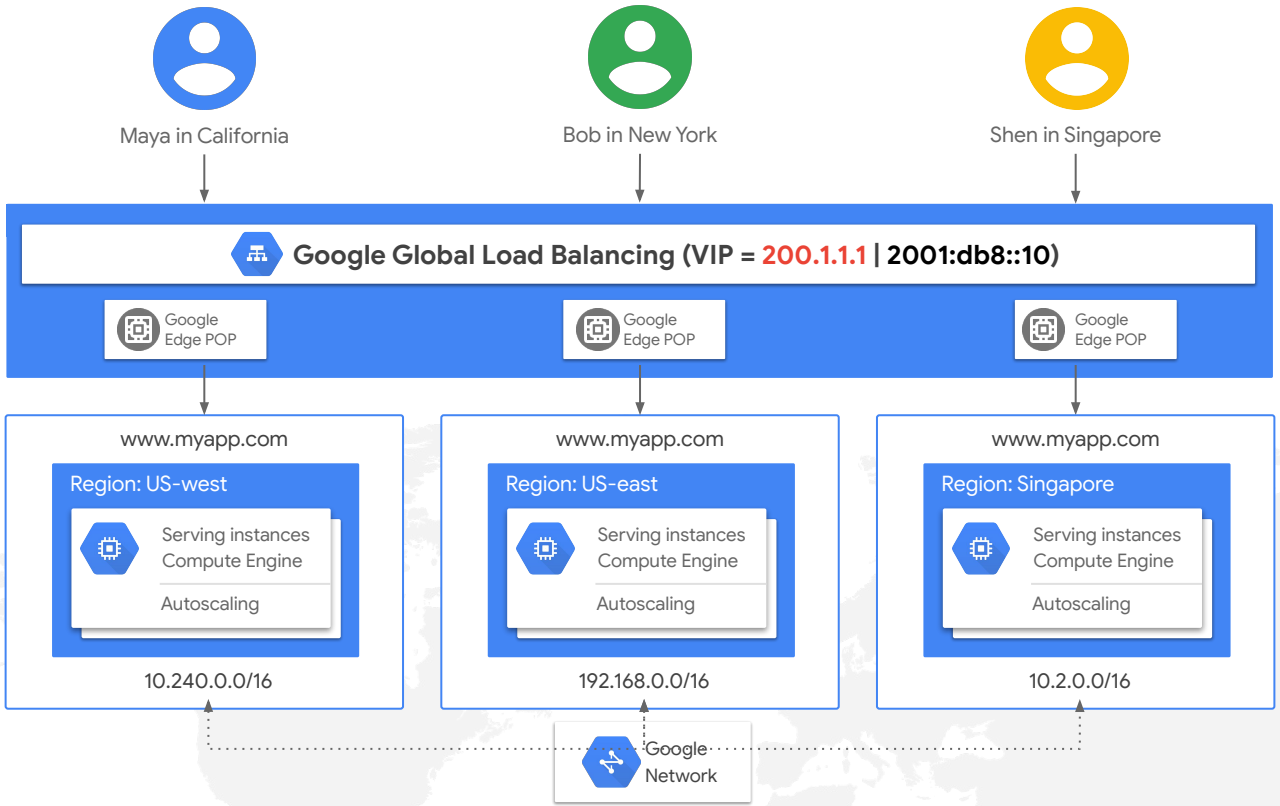
Load balancing types

- High performance
- Fully distributed and software defined
- Regional/zonal spillover and failover
- Intelligent backend autoscaling and health checks

	Type	Geographical scope	Network tiers	Proxy/pass-through
Internal	TCP/UDP	Regional	Premium	Pass-through
	HTTP(s)			Proxy
External	TCP/UDP	Regional	Standard / Premium	Pass-through
	HTTP(s) TCP Proxy SSL Proxy	Regional / Global depending on network tier	Standard / Premium	Proxy

Cloud DNS

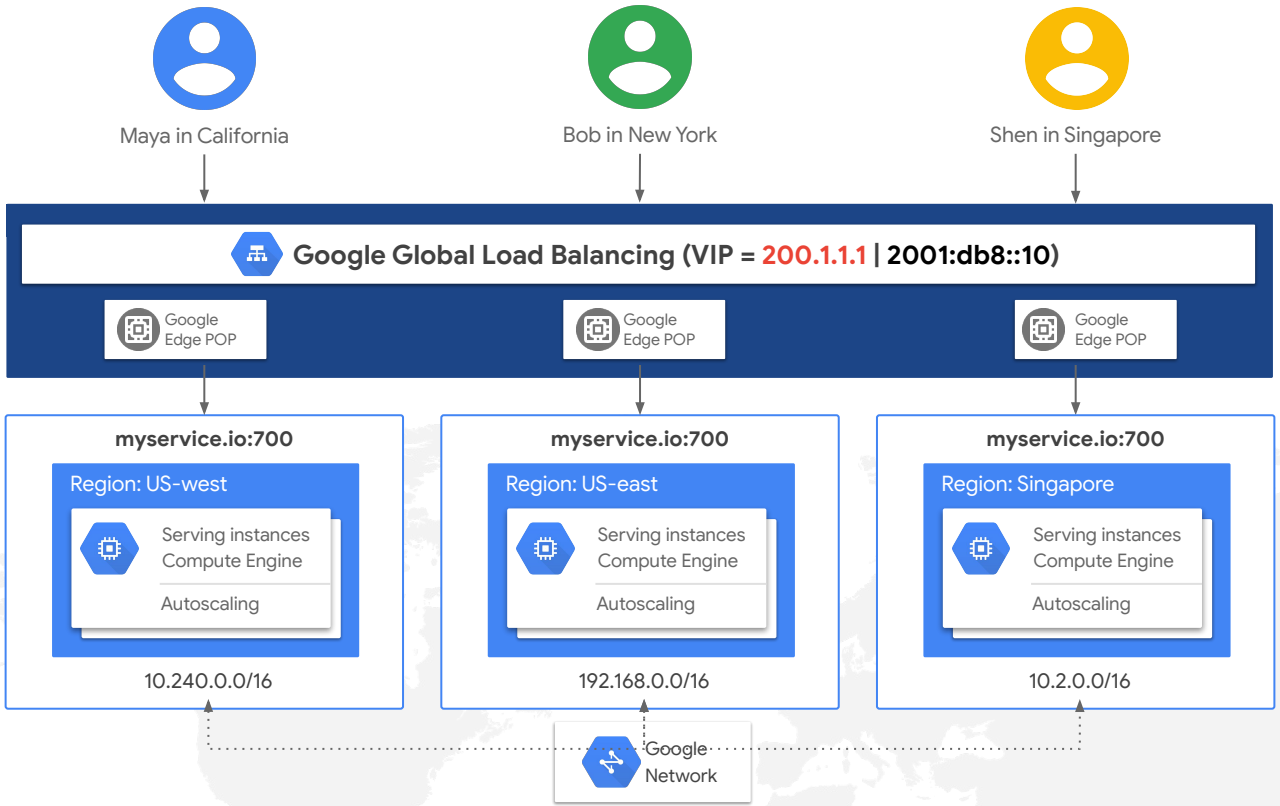
External global HTTP(s) load balancing



- Global anycast IP address
- Implemented on top of Google Front End (GFE)
- Multi-regional load balancing
- Balancing mode: Rate, utilization
- Session affinity: Client IP, generated cookie
- WebSocket support
- Terminates HTTPs traffic. Backend traffic encryption supported.
- DDOS protection (L4)
- Integration with Cloud CDN and Cloud Armor (WAF)

Cloud DNS

External global TCP/SSL load balancing

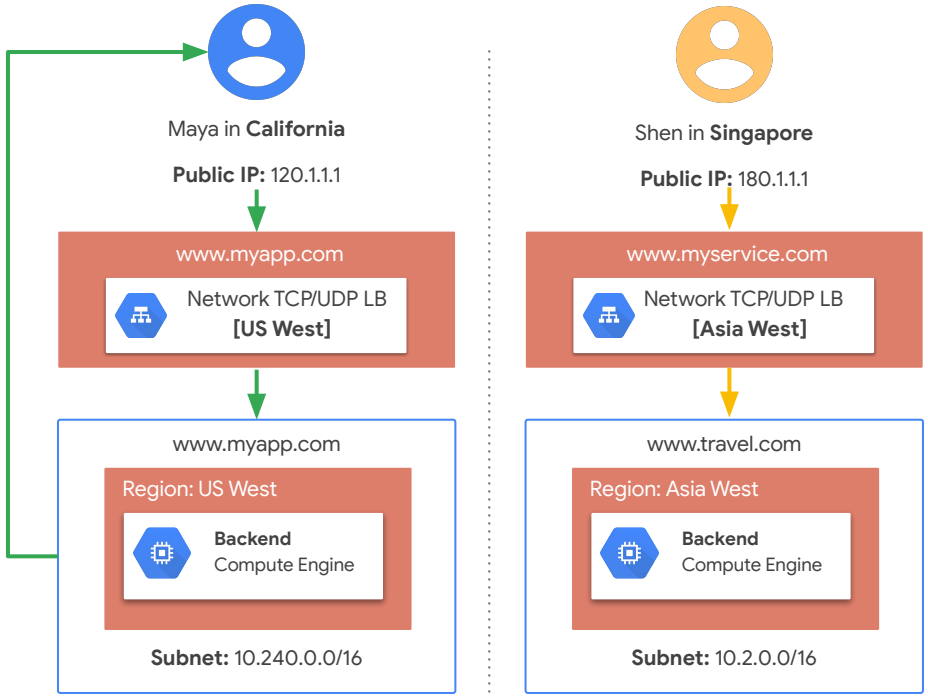


- Global anycast IP address
- Implemented on top of GFE
- Multi-regional load balancing
- Session affinity: Client IP
- DDOS protection (L4)
- SSL proxy for TCP traffic with SSL offload (non-HTTPS encrypted traffic)
- TCP proxy for TCP traffic with SSL offload (non-HTTP unencrypted)
- Requests are load balanced over ports 25, 43, 110, 143, 195, 443, 465, 587, 700, 993, 995, 1883, and 5222

External regional TCP/UDP load balancing

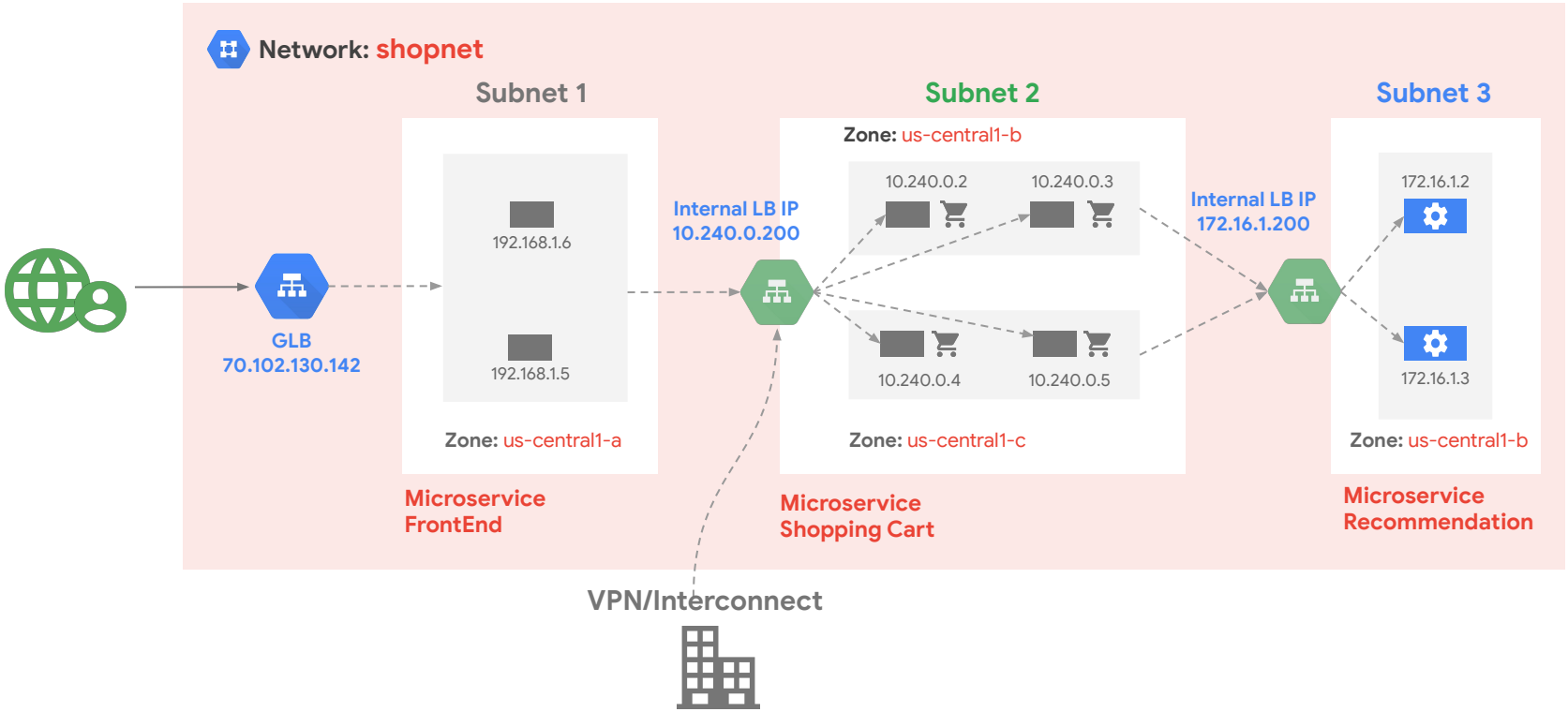
Cloud DNS

Direct Server Return (DSR)



- Also called Network Load Balancer
- Load balancing based on 5-tuple
- Regional
- Pass-through (client IP preserved)
- Session affinity: 2-tuple, 3-tuple, 5-tuple (default)
- Use for UDP/TCP/SSL traffic on ports not supported by the SSL/TCP Proxy load balancers

Internal TCP/UDP (L4) load balancing



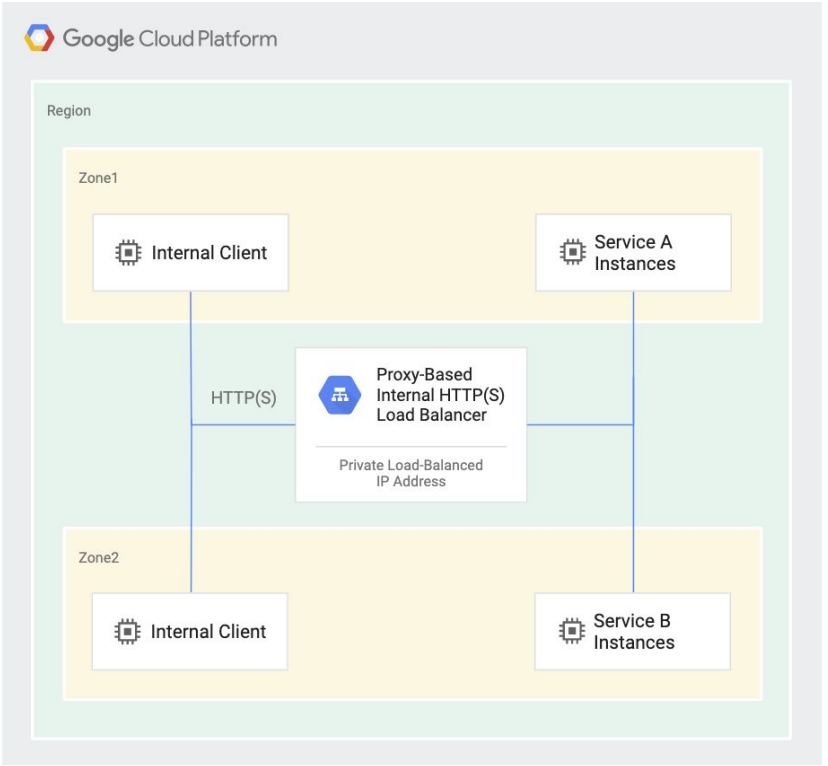
Internal HTTP/HTTPS (L7) load balancing

Modern Envoy-based LB delivered as middle proxy

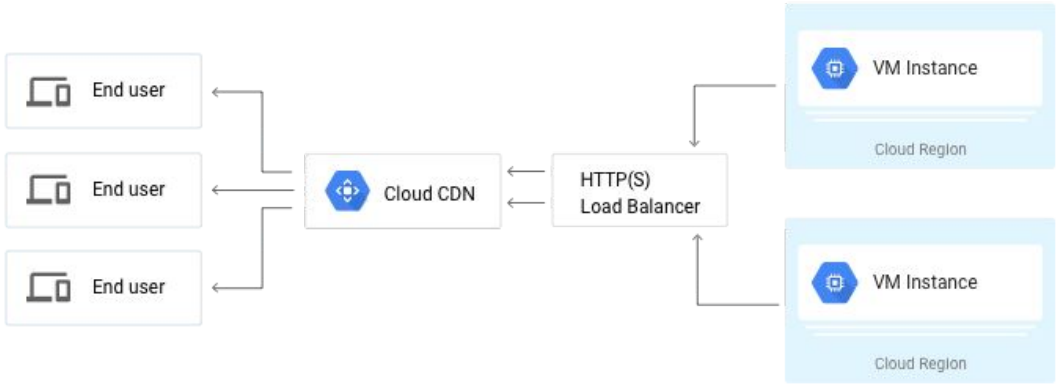
- Regional
- Health checks
- Traffic management rules (URL map)

Rich traffic management

- Route based on HTTPs parameters
- Request/response-based actions
- Advanced load balancing algorithms



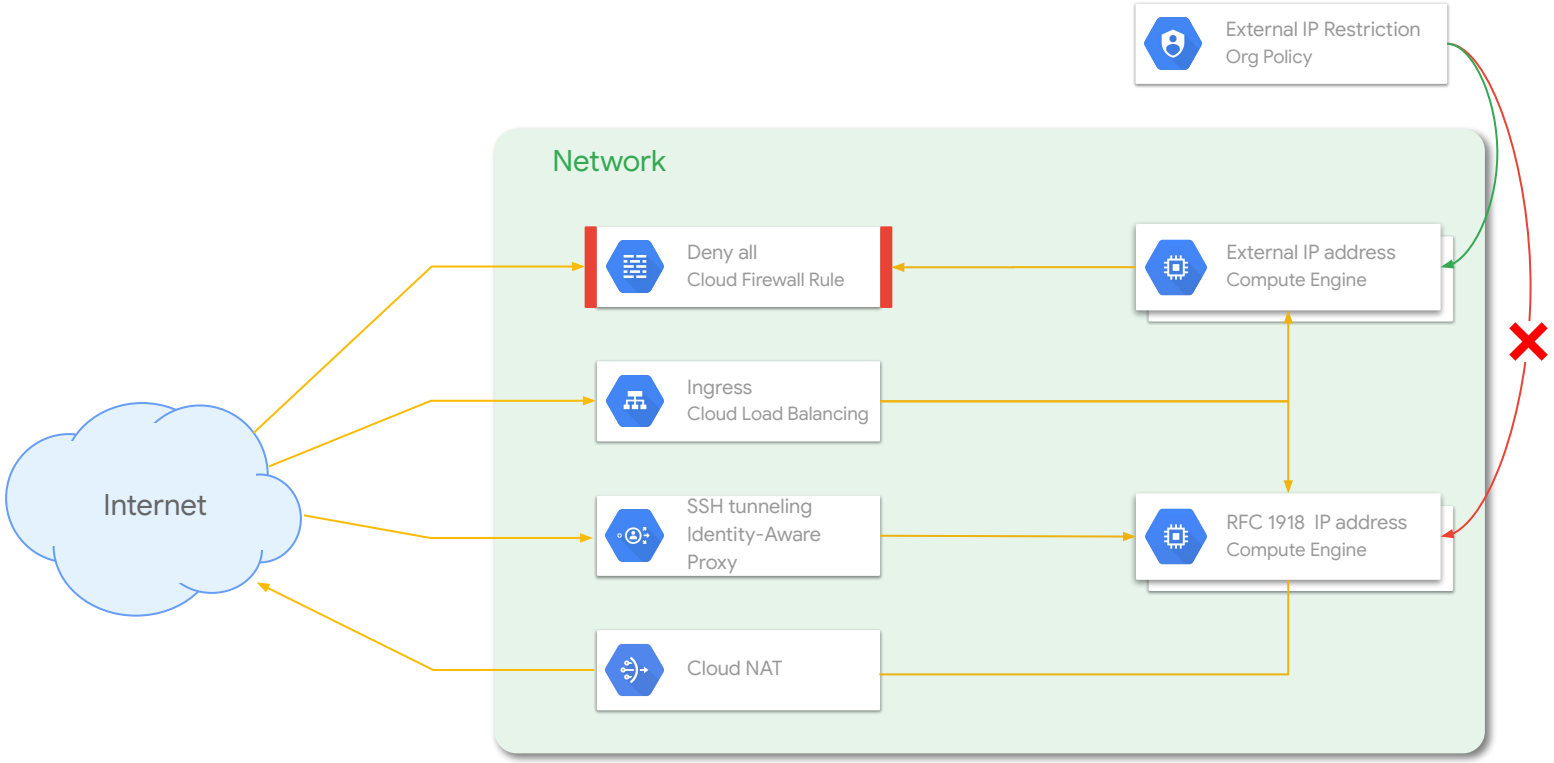
Cloud CDN



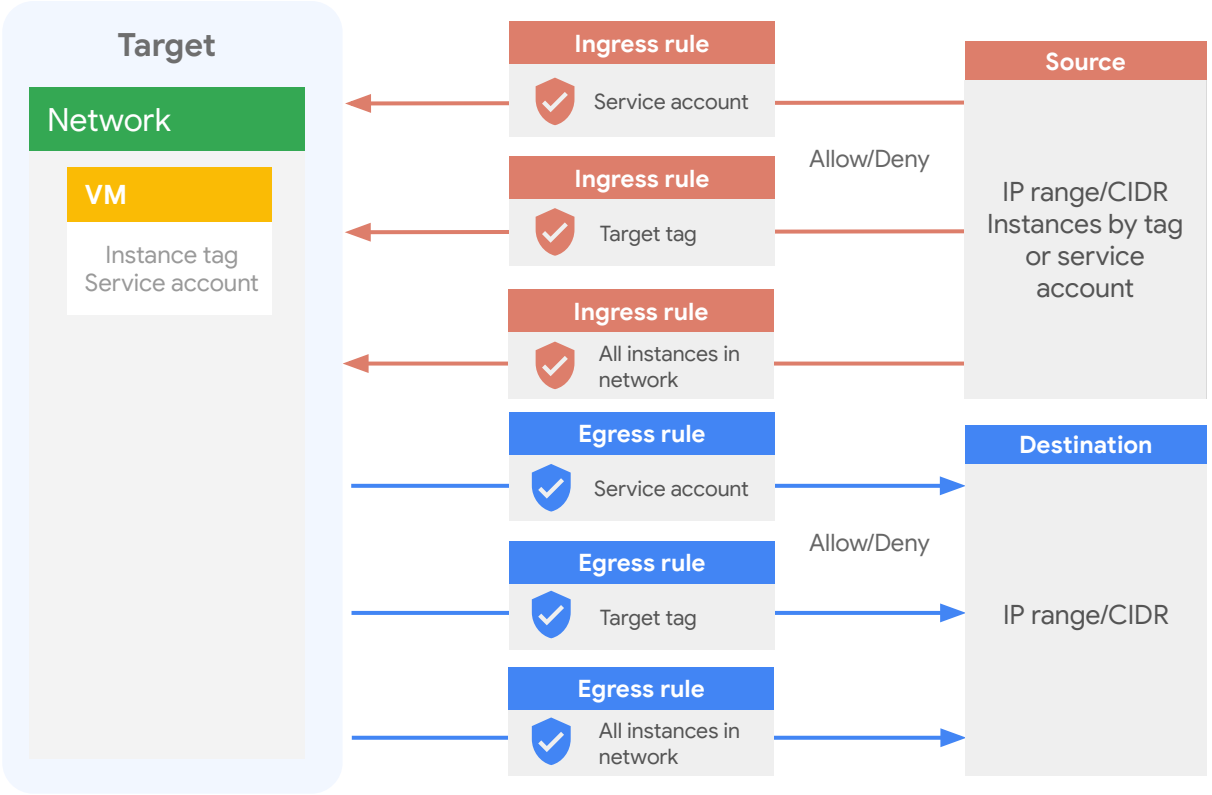
- Uses Google's globally distributed PoP's to **cache HTTP(S) load balanced content** close to your users
- Caches content from **instances** and **storage buckets**
- **90+ locations**, with **single IP** across multiple regions.

Networking access control

Controlling external surfaces



VPC firewall



VPC firewall

- **Stateful** with connection tracking
- **Distributed**: enforced on underlying host

Controls paths

- VM <-> VM
- VM <-> Internet
- VM <-> On-prem

Implied rules

- Ingress deny
- Egress allow

Attaching firewall rules to VMs

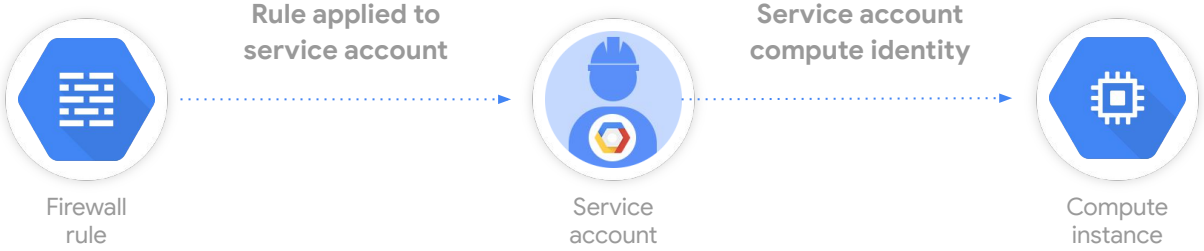
Tags

- Multiple tags applied to one VM (64 max)
- Firewall rule may target multiple tags
- May update tags to live VM

Best practice

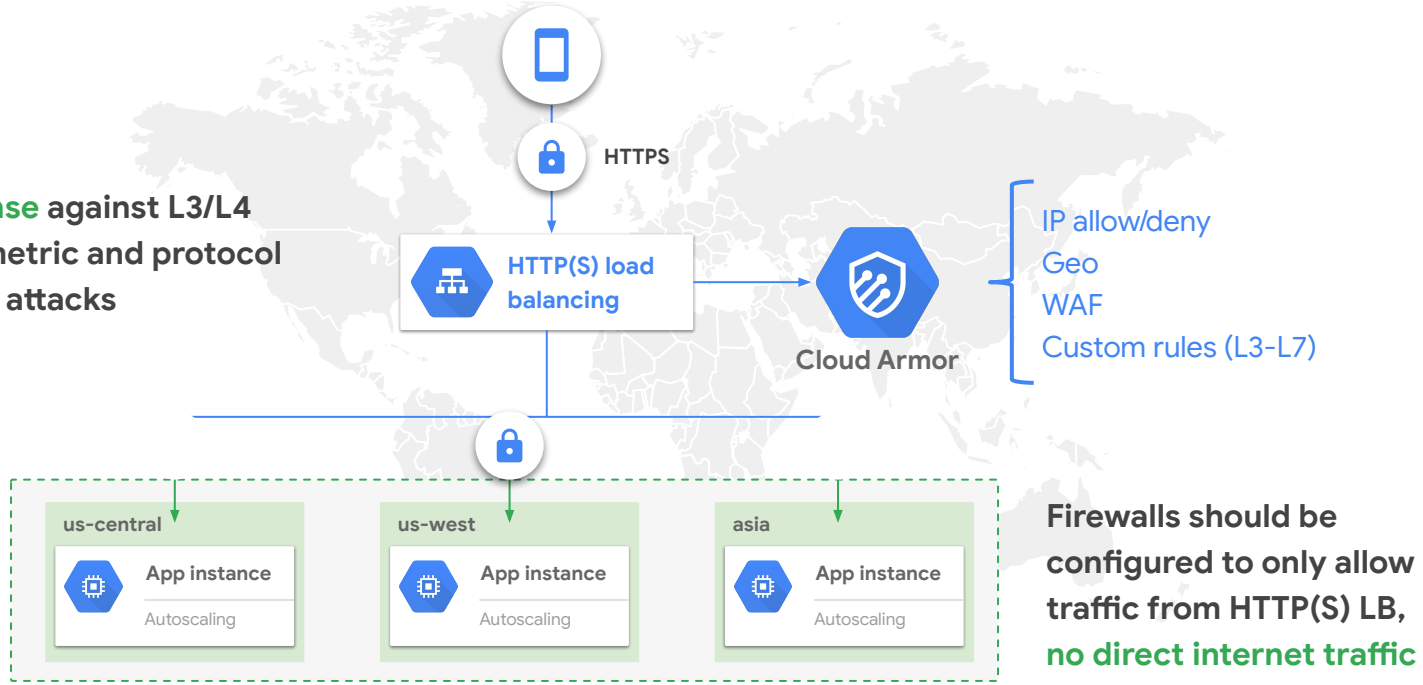
Service accounts

- May restrict who uses
- Must shut down VM to change service account



Cloud Armor: DDoS protection and WAF

Defense against L3/L4 volumetric and protocol DDoS attacks



Firewalls should be configured to only allow traffic from HTTP(S) LB, **no direct internet traffic**

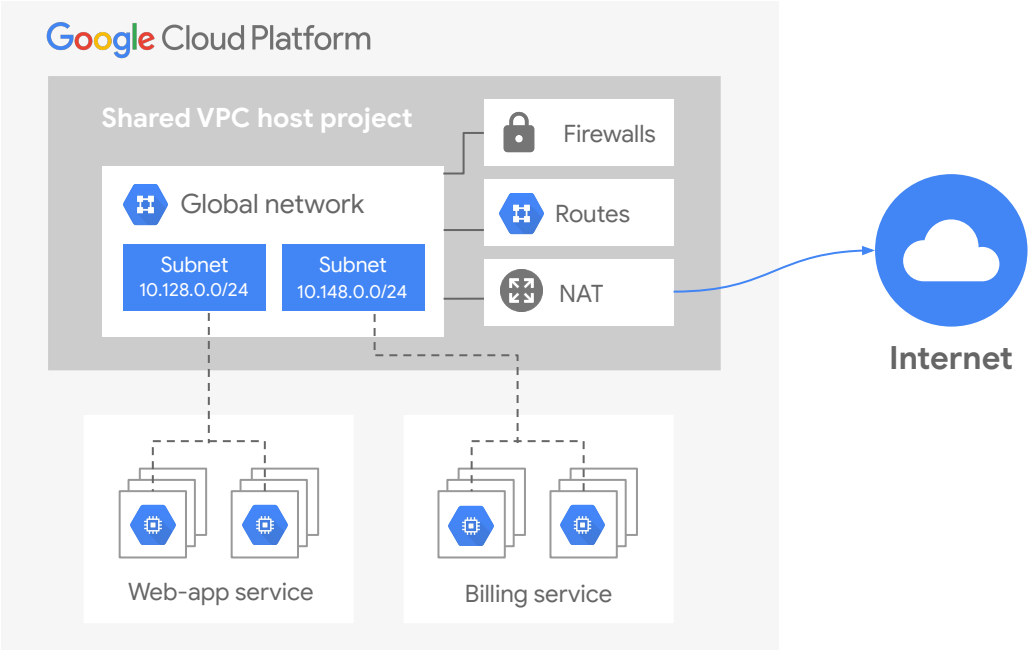
Cloud NAT

Managed NAT solution

Improved security, only outbound connections to the Internet

Scales seamlessly

- Static IPs
- Auto-allocated IPs
- Not proxy based, single NAT gateway scales to thousands of VMs in a region



Define a security perimeter with VPC Service Controls

Define security perimeters around sensitive data in Google Cloud Platform services

- Mitigate data exfiltration risks
- Privately access GCP services from on-premises
- Enforce context-aware access from the internet
- Centrally manage security policies

VPC Service Controls versus VPC Firewall

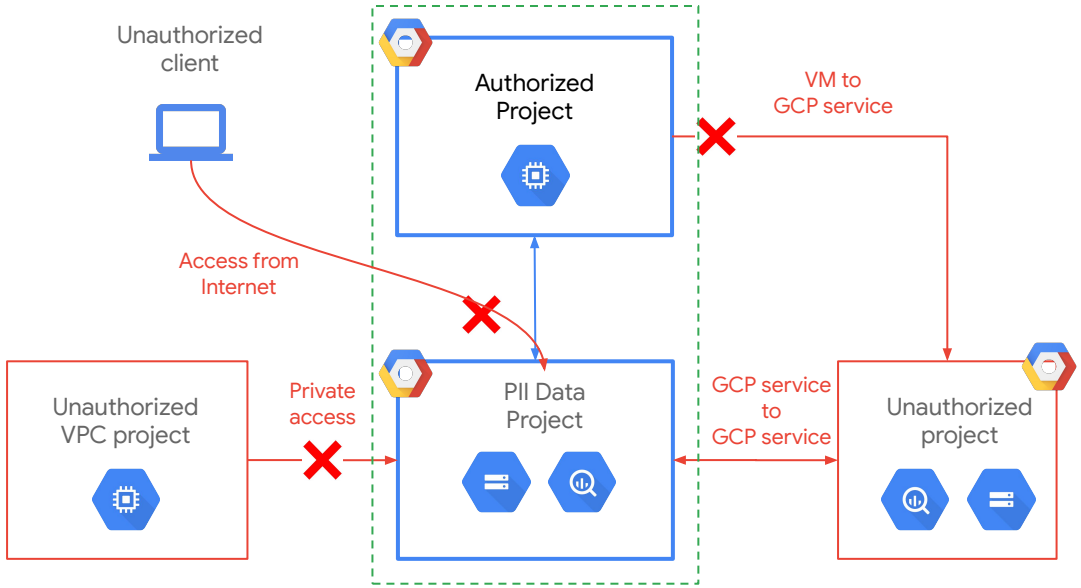
	VPC Firewall	VPC Service control
Control path	VM ⟷ VM VM ⟷ Internet VM ⟷ On-premise	GCP Service ⟷ VM GCP Service ⟷ Internet GCP Service ⟷ On-premise GCP Service ⟷ GCP Service
Conditions	5-tuple VM tags VM service accounts	VPC network GCP project Service accounts Internet IPs
Policies apply to	VMs in a VPC network VMs grouped by tag VMs grouped by service account	API based resources grouped by project

VPC Service Controls

Service perimeter

Extend perimeter security to managed GCP services

- Control VM-to-service and service-to-service paths.
- Ingress: prevent access from the unauthorized networks.
- Egress: prevent copying of data to unauthorized GCP Projects.
- Project level granularity.

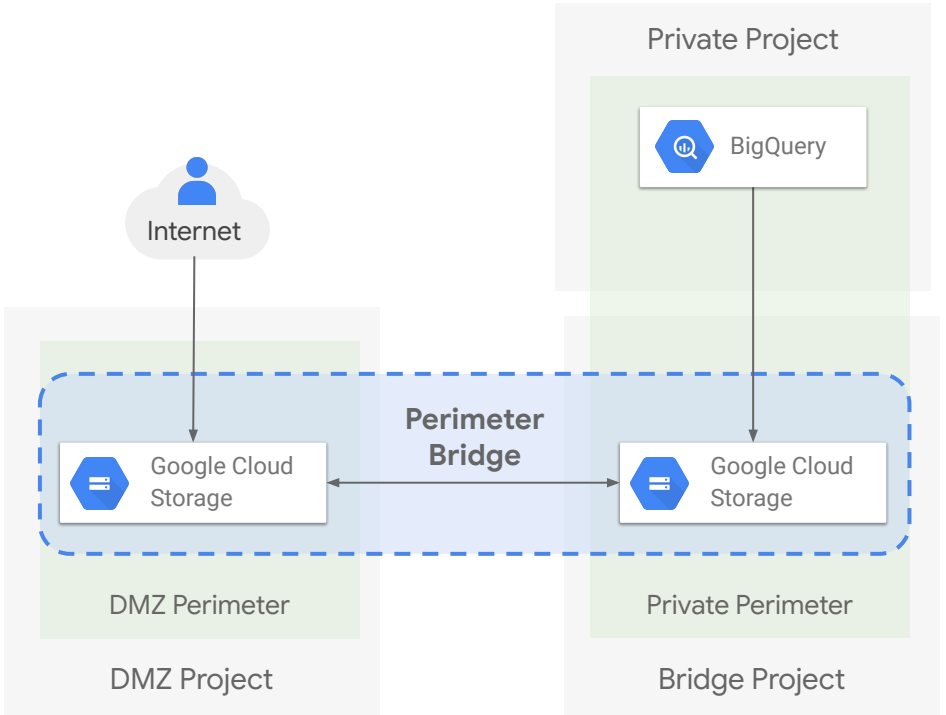


VPC Service controls - Perimeter Bridge

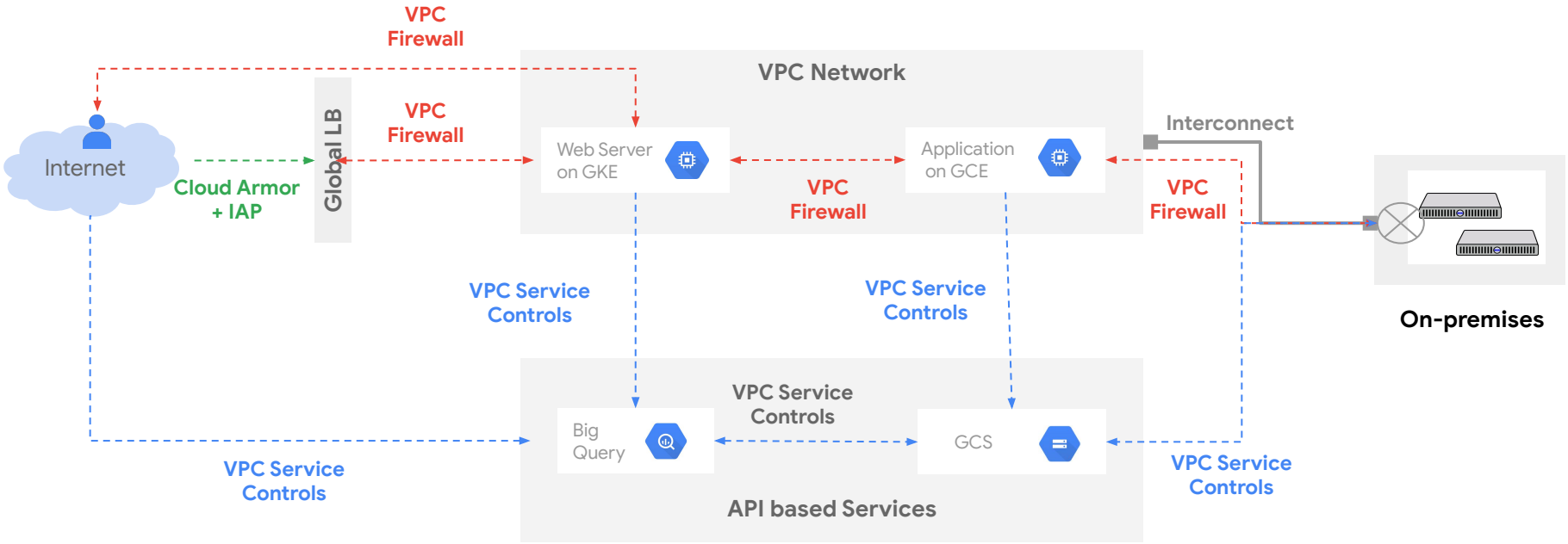
Perimeter Bridge

Share data across Service Perimeters

- Allows communication between GCP resources across Service Perimeters.
- A GCP project can belong to only one Service Perimeter but can be a part of multiple Perimeter Bridges.
- Only the Service Perimeter determines the security policies for a Project.



VPC Service Controls - Example architecture



Identity-aware proxy

Central enforcement

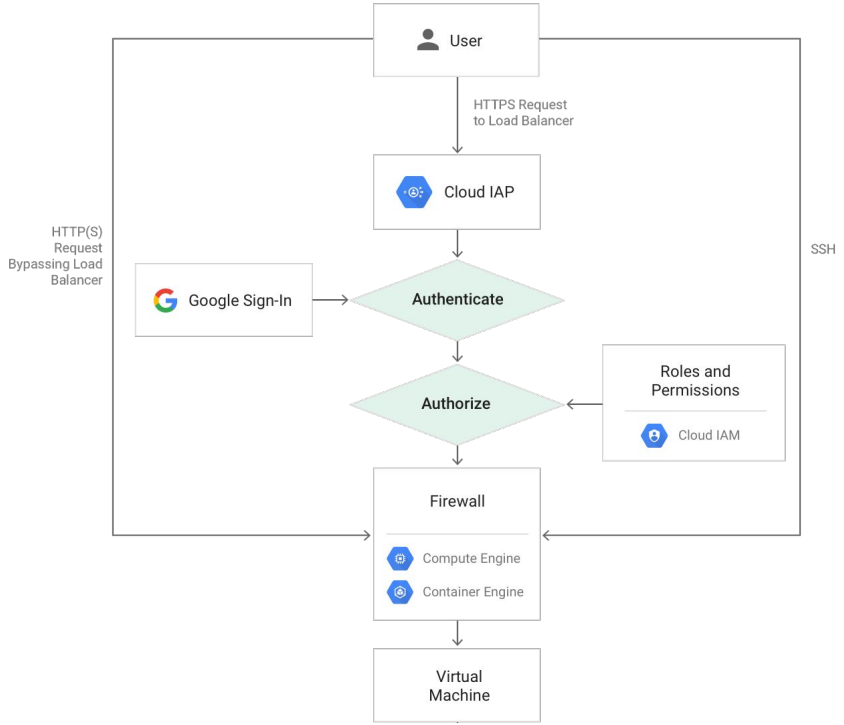
- Single point of control for managing user access
- Security team can define and enforce policy

Access control

- Control access by user identity
- Apply policy by group membership
- Supports 2FA Security Keys

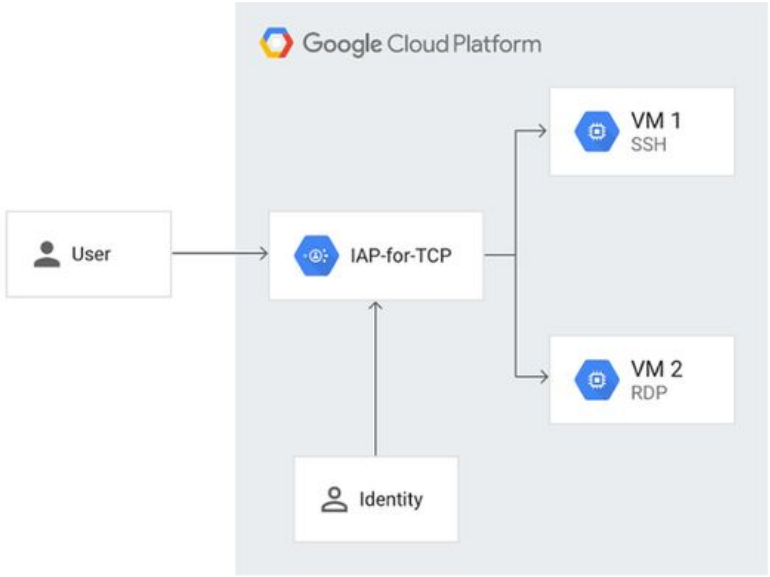
Deployment

- Little to no change to applications
- No need to implement own authentication for each application
- Integrated with HTTP(s) Load Balancer



Identity-aware proxy for TCP

- Tunnel TCP traffic to instances without exposing them to the public internet
- Traffic between client and IAP is wrapped in HTTPS
- Access controlled by user identity and IAM



SSH Common pattern

- IAP for TCP can be easily used instead of a bastion host by using Cloud SDK:

  gcloud compute ssh user@instance --zone <zone>

Network logging

VPC Flow Logs

VPC Firewall

HTTP(s) Load Balancer (Beta)

Cloud CDN (Beta)

Cloud NAT

Cloud DNS

Mitigating DDoS attacks

Mitigating DDoS attacks is a shared responsibility between Google and you. You should consider:

Attack surface	Reduce the attack surface on Google Cloud Platform by reducing externally facing resources
Internal traffic	Isolate internal traffic from the outside world
Load balancing	Use proxy-based load balancing to distribute load across resources
Scaling	Ensure that your apps scale well to handle the increased load
CDN offloading	Offload static content to a CDN (such as Cloud CDN) to minimize impact
DDoS protection	Deploy DDoS protection (such as Cloud Armor) if necessary
Rate limits and quotas	Be aware of the role API rate limits and resource quotas play in protection against DDoS

Key decisions

1. How will cloud resources communicate with each other?
2. How will resources be segmented into networks and subnets?
3. What are the scalability requirements concerning networking components?
4. How will name resolution be solved among cloud resources, and between the cloud and connected environments?
5. What strategies will be used to connect GCP with corporate networks?
6. How will cloud resources communicate with the internet?

Key decisions

1. How will cloud resources communicate with each other?
2. How will resources be segmented into networks and subnets?
3. What are the scalability requirements concerning networking components?
4. How will name resolution be solved among cloud resources, and between the cloud and connected environments?
5. What strategies will be used to connect GCP with corporate networks?
6. How will cloud resources communicate with the internet?

Multiple VPC Networks

1 hour 10 minutes 7 Credits Rate Lab

https://www.qwiklabs.com/focuses/22772?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%7D&parent=catalog&search_id=15442932

GSP211

Google Cloud Self-Paced Labs

Networking in the Google Cloud ♡

Fundamental 6 Steps 7 hours 38 Credits

Networking is a principle theme of cloud computing. It's the underlying structure of Google Cloud, and it's what connects all your resources and services to one another. This fundamental-level quest will cover essential Google CLoud networking services and will give you hands-on practice with specialized tools for developing mature networks. From learning the ins-and-outs of VPCs, to creating enterprise-grade load balancers, Networking in the Google Cloud will give you the practical experience needed so you can start building robust networks right away. Looking for a hands on challenge lab to demonstrate your skills and validate your knowledge? On completing this quest, enroll in and finish the additional challenge lab at the end of the Build and Secure Networks in Google Cloud Quest to receive an exclusive Google Cloud digital badge.

Infrastructure Security

https://www.qwiklabs.com/quests/31?catalog_rank=%7B%22rank%22%3A1%2C%22num_filters%22%3A0%2C%22has_search%22%3Atrue%7D&search_id=8829218

Assignment

https://www.qwiklabs.com/focuses/1232?parent=catalog

HTTP Load Balancer with Cloud Armor

1 hour 7 Credits ★★★★☆

GSP215

Google Cloud Self-Paced Labs