The information in this presentation is classified:

Google confidential & proprietary

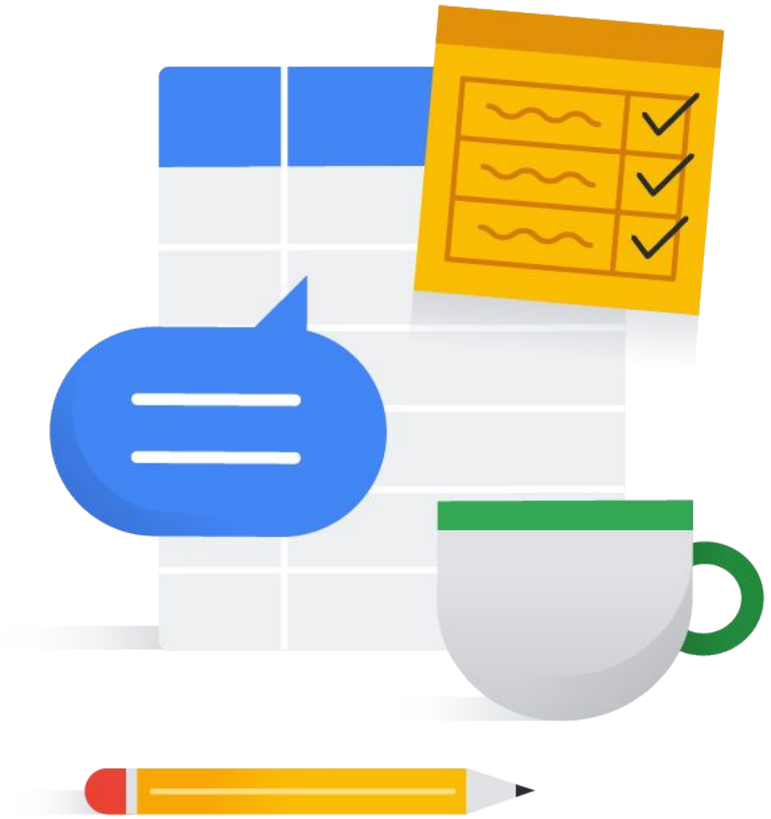
⚠️ This presentation is shared with you under NDA.

- Do **not** record or take screenshots of this presentation.
- Do **not** share or otherwise distribute the information in this presentation with anyone **inside** or **outside** of your organization.

Thank you!

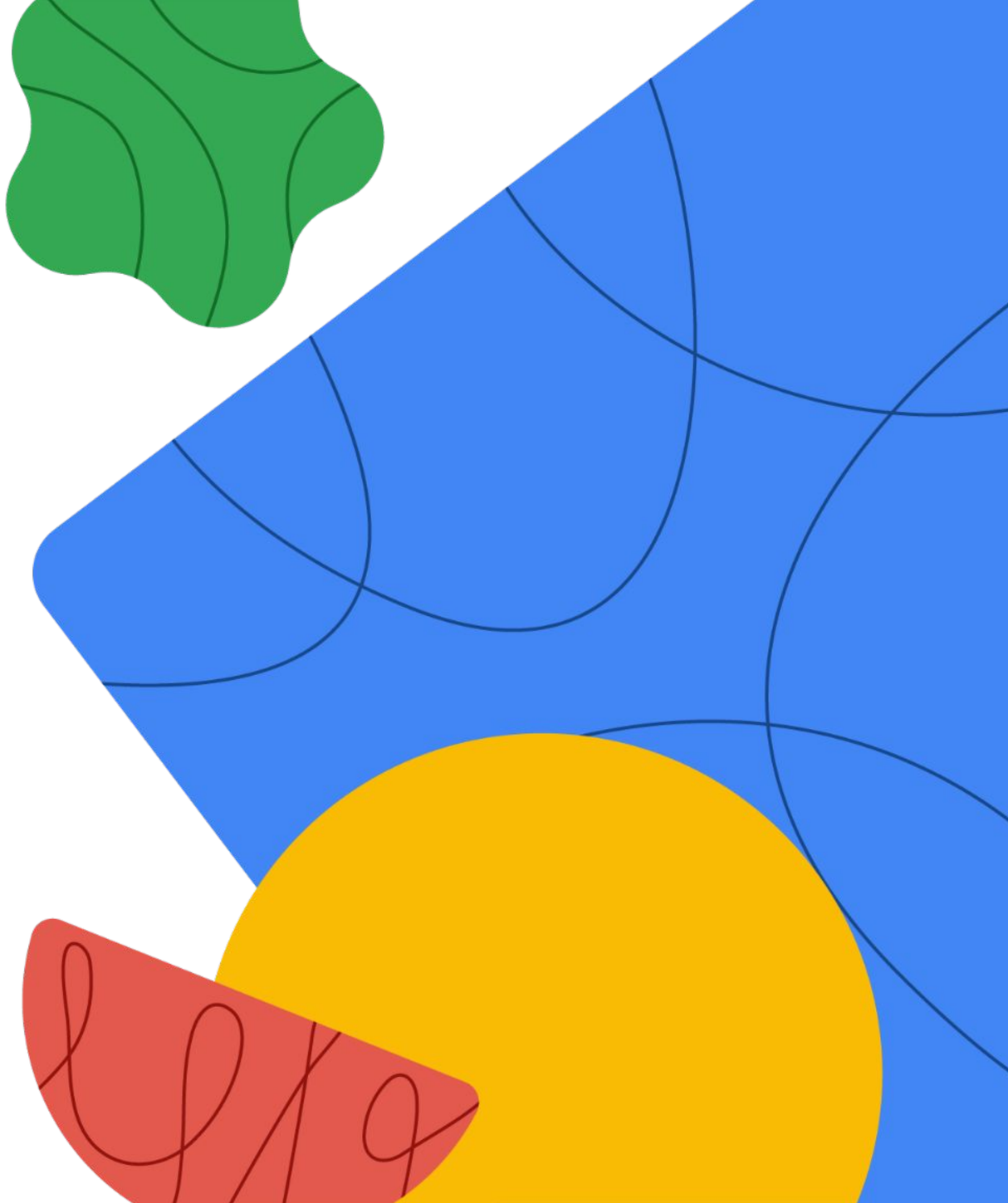
Program issues or concerns?

- Problems with **accessing** Cloud Skills Boost for Partners
  - cloud-partner-training@google.com
- Problems with **a lab** (locked out, etc.)
  - support@qwiklabs.com



Google Cloud

Network Security



Our agenda

01 Google Cloud VPC networking fundamentals

02 Sharing networks across projects

03 Load Balancing

04 Hybrid connectivity

05 Networking design and deployment

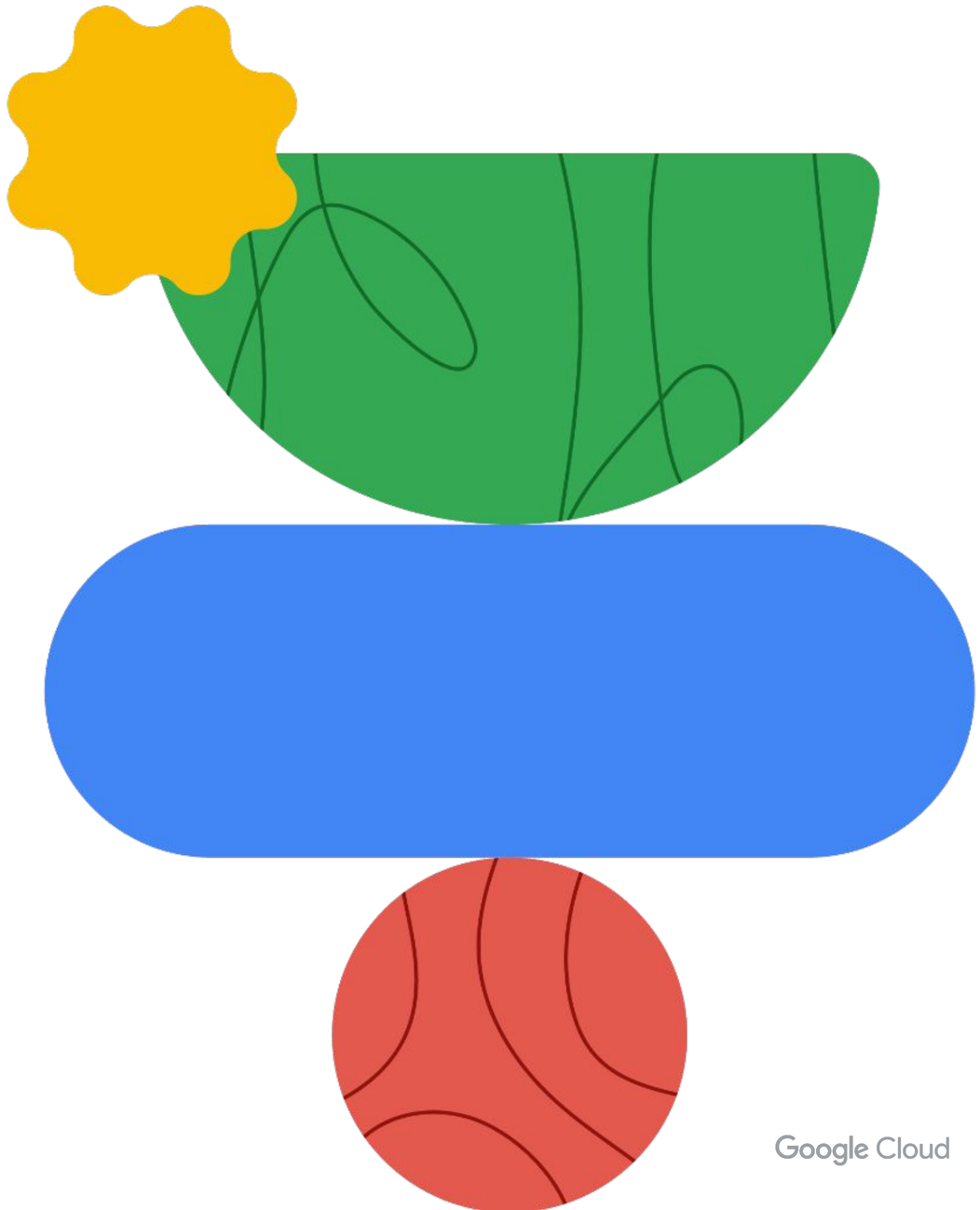
Objectives

01 Discuss Google Cloud networking fundamentals.

02 Identify common network designs in Google Cloud.

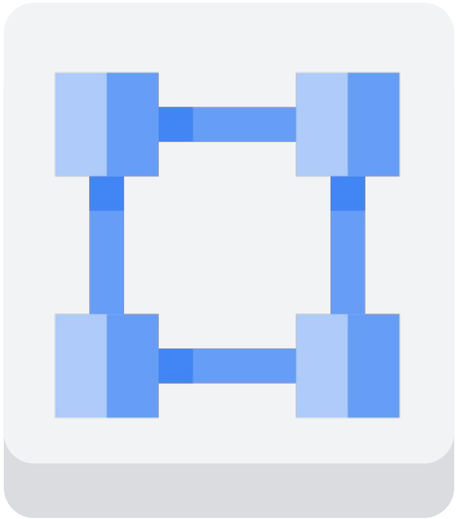
03 Describe the major network security mechanisms in Google Cloud.

Google Cloud VPC Networking Fundamentals



VPC objects

- Google Cloud lets you provision, connect, and isolate your Google Cloud resources within a Virtual Private Cloud.
- You can also define granular networking policies within Google Cloud, and between Google Cloud and on-premises or other public cloud environments.
- VPC is a comprehensive set of Google-managed networking objects.

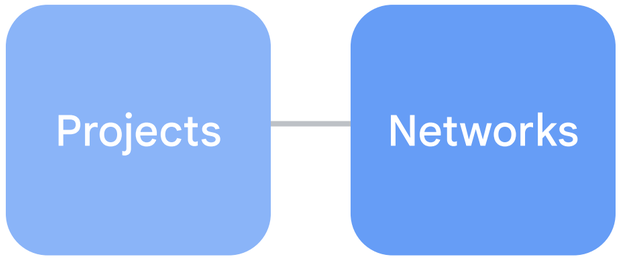


VPC projects

Projects

Projects encompass all the services used within the Google Cloud platform, including networks.

VPC projects



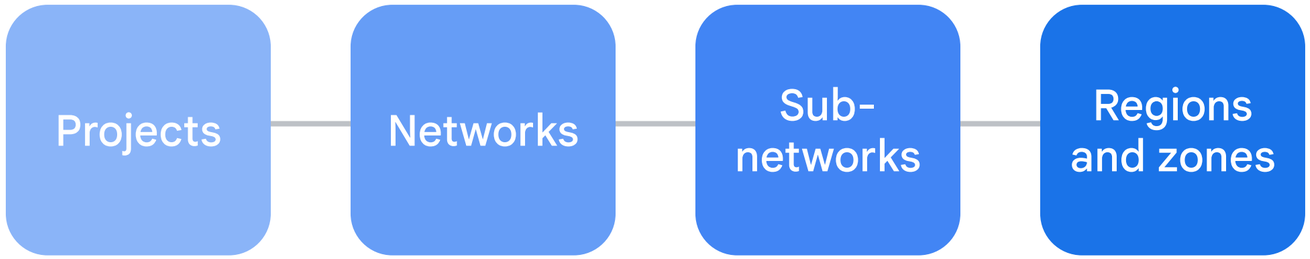
Networks exist in three different modes:

- **Default mode:** Automatically created for each project, offering basic functionality.
- **Auto mode:** Provides basic networking with limited customization.
- **Custom mode:** Offers advanced networking and granular control.

VPC projects

Subnetworks allow users to divide or segment their network into smaller, more manageable units. This helps to isolate different parts of the network and improve security.

VPC projects

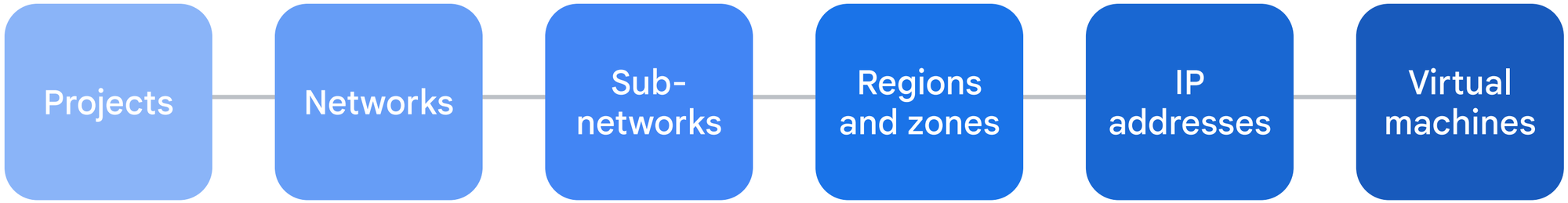


- Regions represent the Google data centers, which are large geographical areas that host multiple zones.
- Zones are smaller, isolated locations within a region that provide continuous data protection and high availability.

VPC projects

- VPC provides both internal and external IP addresses for resources within the network.
- It also offers granular control over IP address range selection, allowing users to allocate specific IP ranges to different parts of their network.

VPC projects



- VMs are the fundamental computing units in Google Cloud.
- In the context of networking, we will focus on configuring VM instances to connect to and communicate with other resources within the VPC network.

VPC projects

- Routes control how traffic is forwarded within a VPC network and to external destinations.
- Firewall rules define security policies for allowing or denying traffic based on various criteria such as source, destination, and port.

Projects and networks

Project

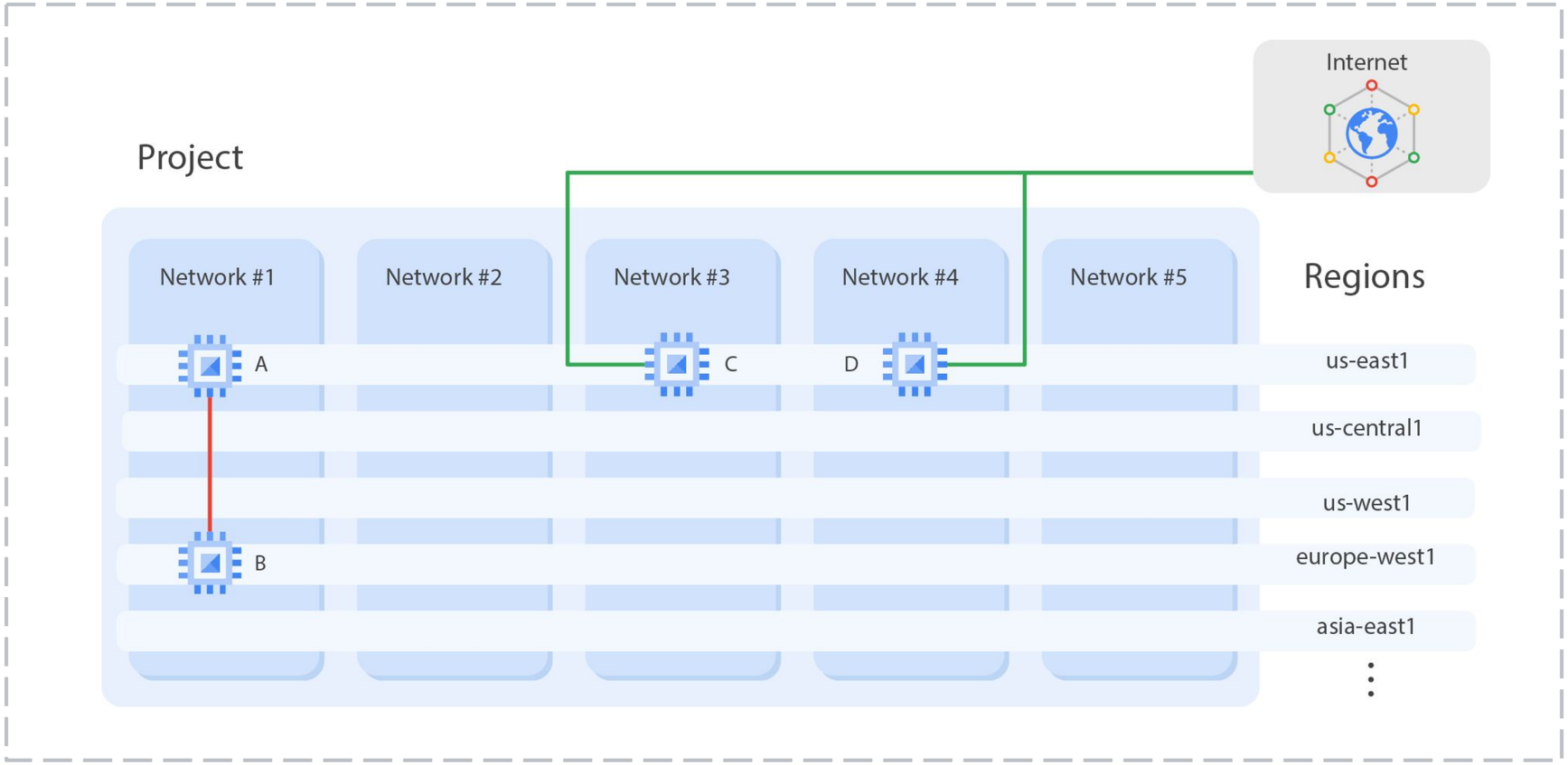
- Associates objects and services with billing
- Contains networks (up to 5)
- Networks can be shared/peered

Network

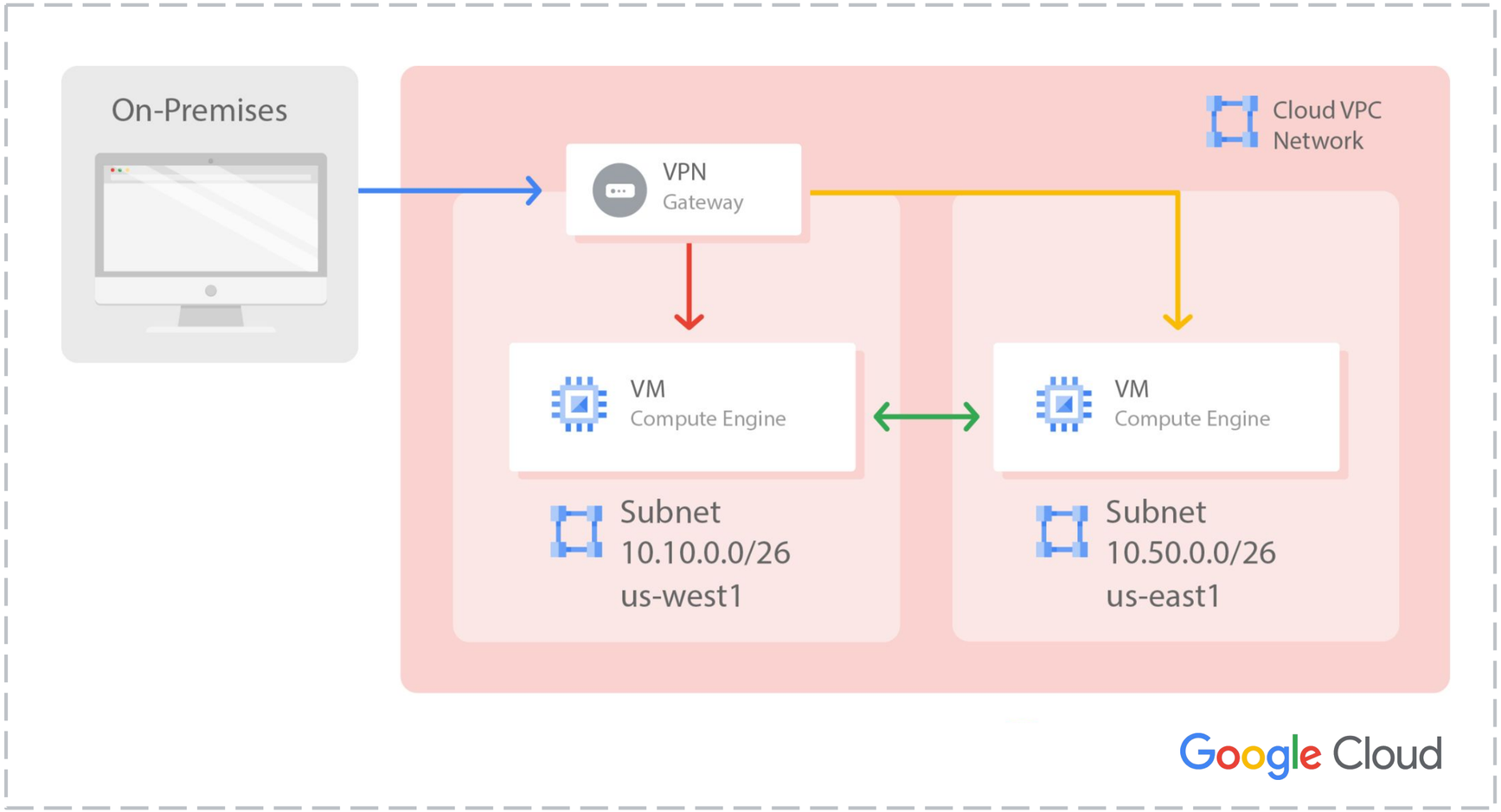
- No IP address range
- Global and spans all available regions
- Contains subnetworks
- Type: default, auto, or custom

Network isolate systems

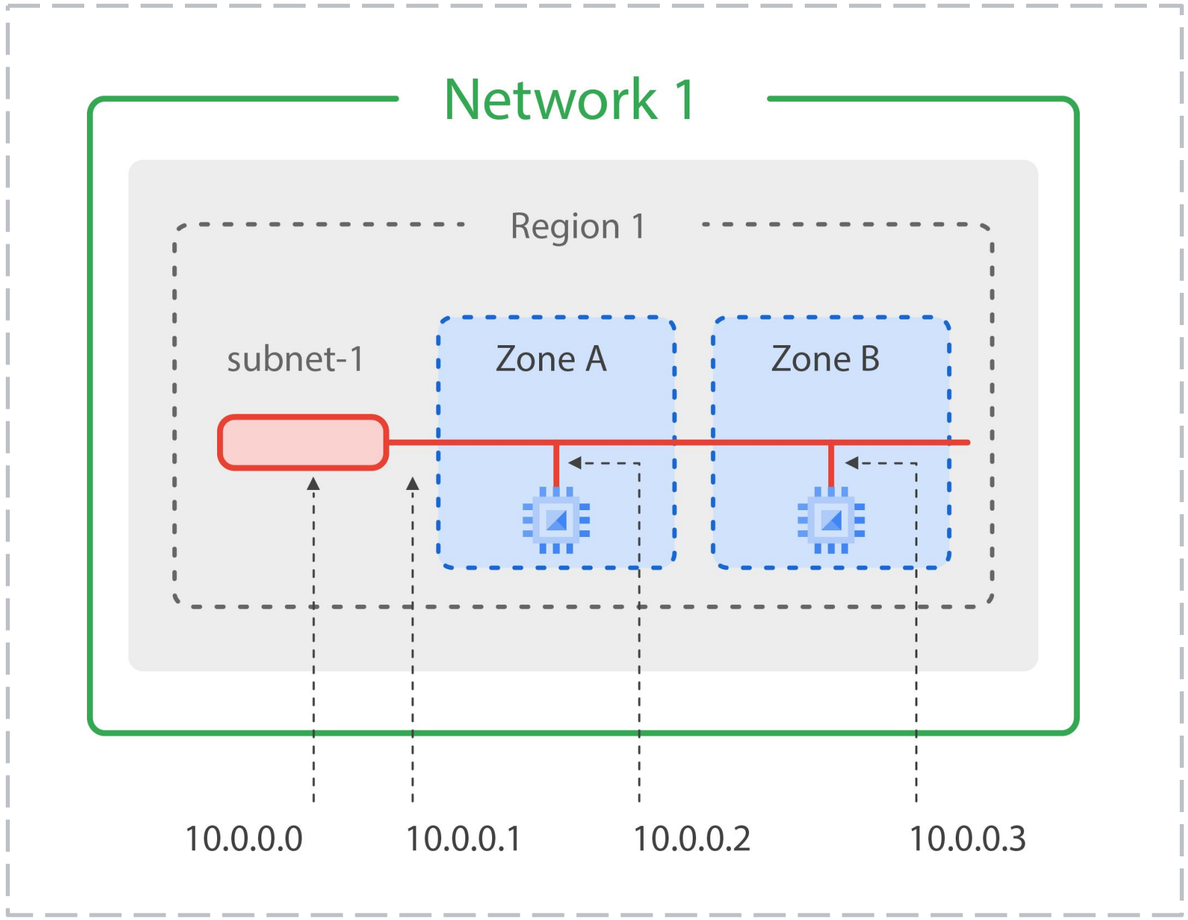
- **A** and **B** can communicate over internal IPs even though they are in different regions.
- **C** and **D** must communicate over external IPs even though they are in the same region.



Google's VPC is global



Subnetworks cross zones



- VMs can be on the same subnet but in different zones.
- A single firewall rule can apply to both VMs.

VMs can have internal and external IP addresses

Internal IP

- Allocated from subnet range to VMs by DHCP
- DHCP lease is renewed every 24 hours
- VM name + IP is registered with network-scoped DNS

External IP

- Assigned from pool (ephemeral)
- Reserved (static)
- Bring Your Own IP address (BYOIP)
- VM doesn't know external IP; it is mapped to the internal IP

DNS resolution for internal addresses

Hostname resolution

Each instance has a hostname that can be resolved to an internal IP address:

- The hostname is the same as the instance name.
- FQDN is [hostname].[zone].c.[project-id].internal.
- Example: guestbook.asia-east1-b.c.guestbook-151617.internal

Internal DNS resolver

Name resolution is handled by internal DNS resolver:

- Provided as part of Compute Engine (169.254.169.254).
- Configured for use on instance via DHCP.
- Provides answer for internal and external addresses.

DNS resolution for internal addresses

External IP addresses

Instances with external IP addresses can allow connections from hosts outside of the project.

- Users connect directly using external IP address.
- Admins can also publish public DNS records pointing to the instance.
  - Public DNS records are not published automatically.

Publishing DNS Records Externally

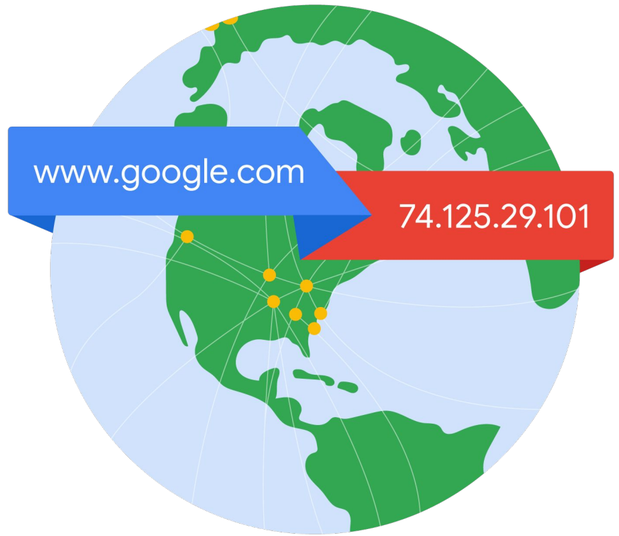
- DNS records for external addresses can be published using existing DNS servers (outside of Google Cloud).

Cloud DNS

- DNS zones can be hosted using Cloud DNS.

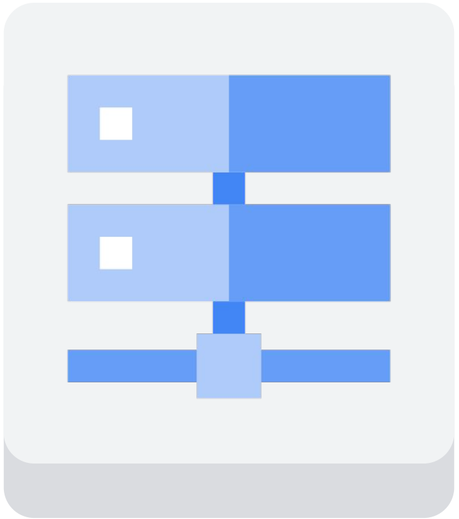
Host DNS zones using Cloud DNS

- Google's DNS service
- Translate domain names into IP address
- Low latency
- High availability (100% uptime SLA)
- Create and update millions of DNS records
- UI, command line, or API



Protect Cloud DNS with DNSSEC

- Protect domains from spoofing and poisoning attacks
- Configure DNSSEC at the:
  - DNS zone level
  - Top Level Domain (TLD) registry
  - DNS resolver



Cloud DNS

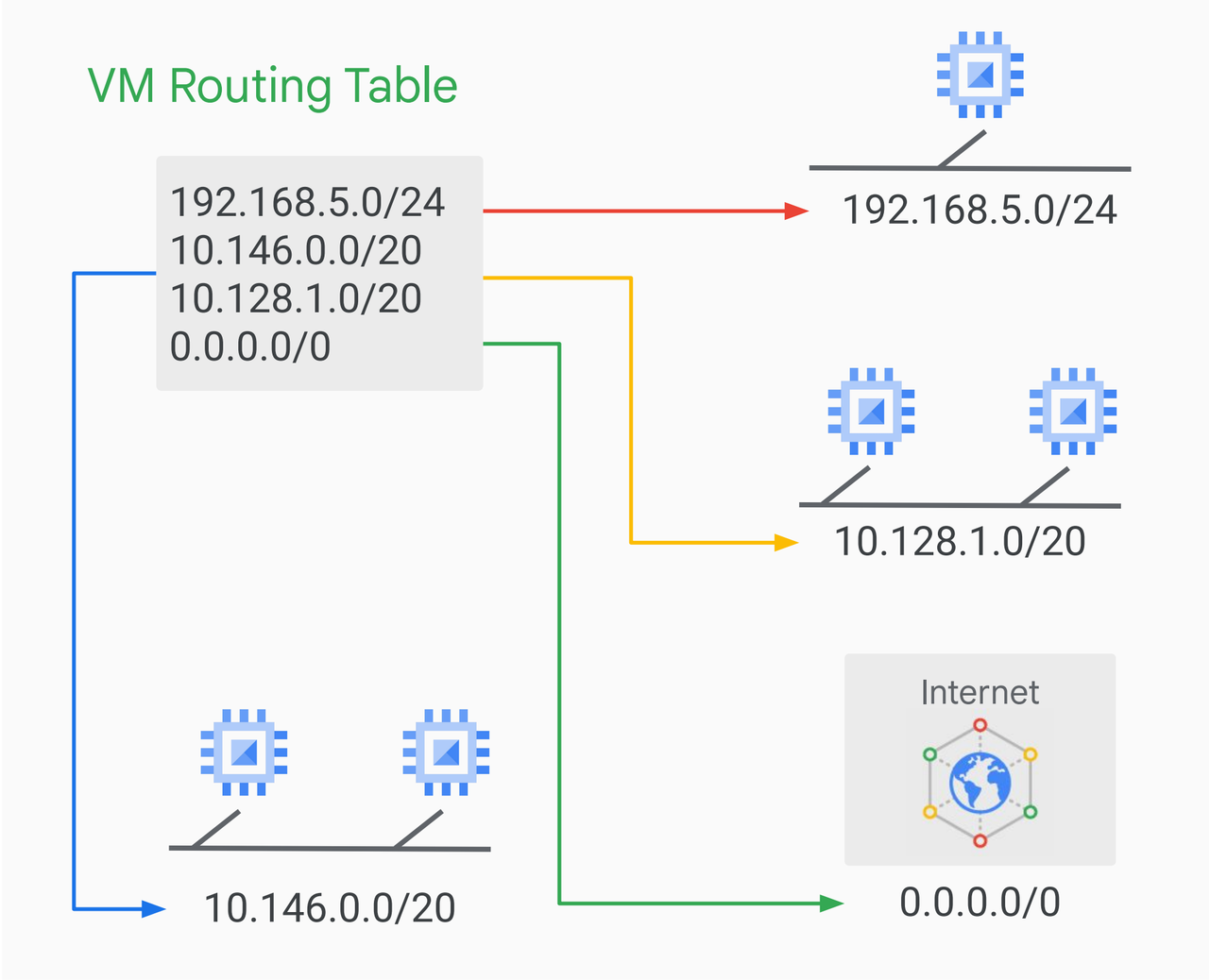
A route is a mapping of an IP range to a destination

- Every network has:
  - Routes that let instances in a network send traffic directly to each other.
  - A default route that directs packets to destinations that are outside the network.
- Firewall rules must also allow the packet.

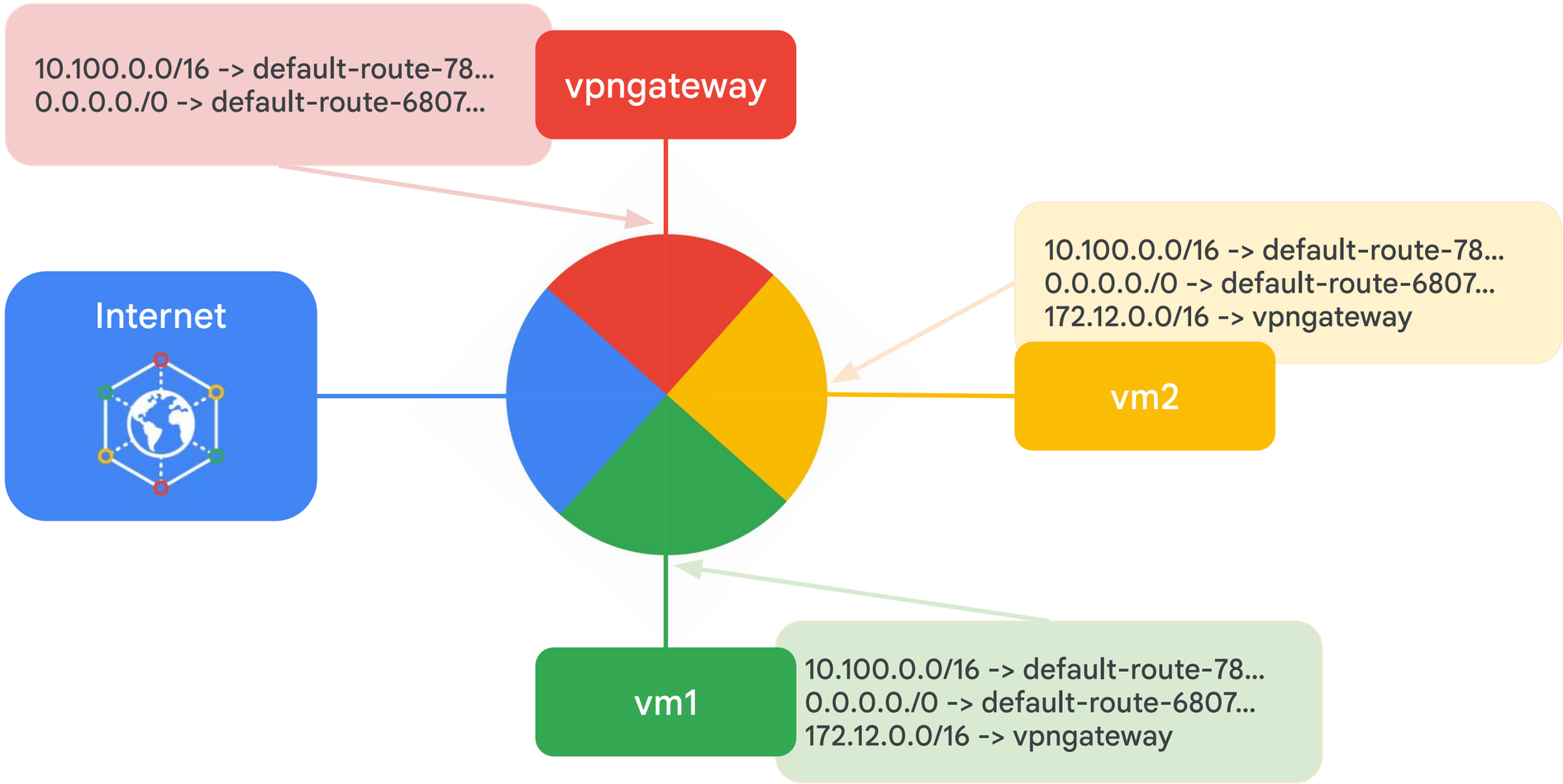
Cloud Routes

Routes map traffic to destination networks

- Destination in CIDR notation
- Applies to traffic egressing a VM
- Forwards traffic to most specific route
- Traffic is delivered only if it also matches a firewall rule
- Created when a subnet is created
- Enables VMs on same network to communicate



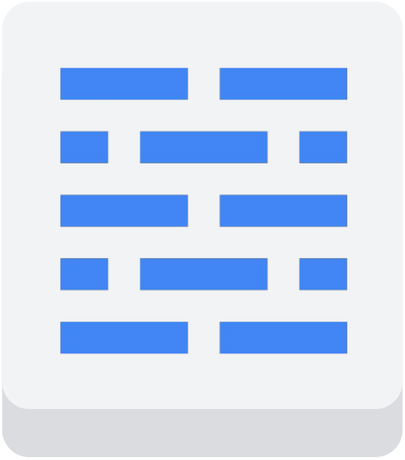
Instance routing tables



Firewall rules

Protect your VM instances from unapproved connections

- VPC network functions as a distributed firewall.
- Firewall rules are applied to the network as a whole.
- Connections are allowed or denied at the instance level.
- Firewall rules are stateful.
- Implied deny all ingress and allow all egress.

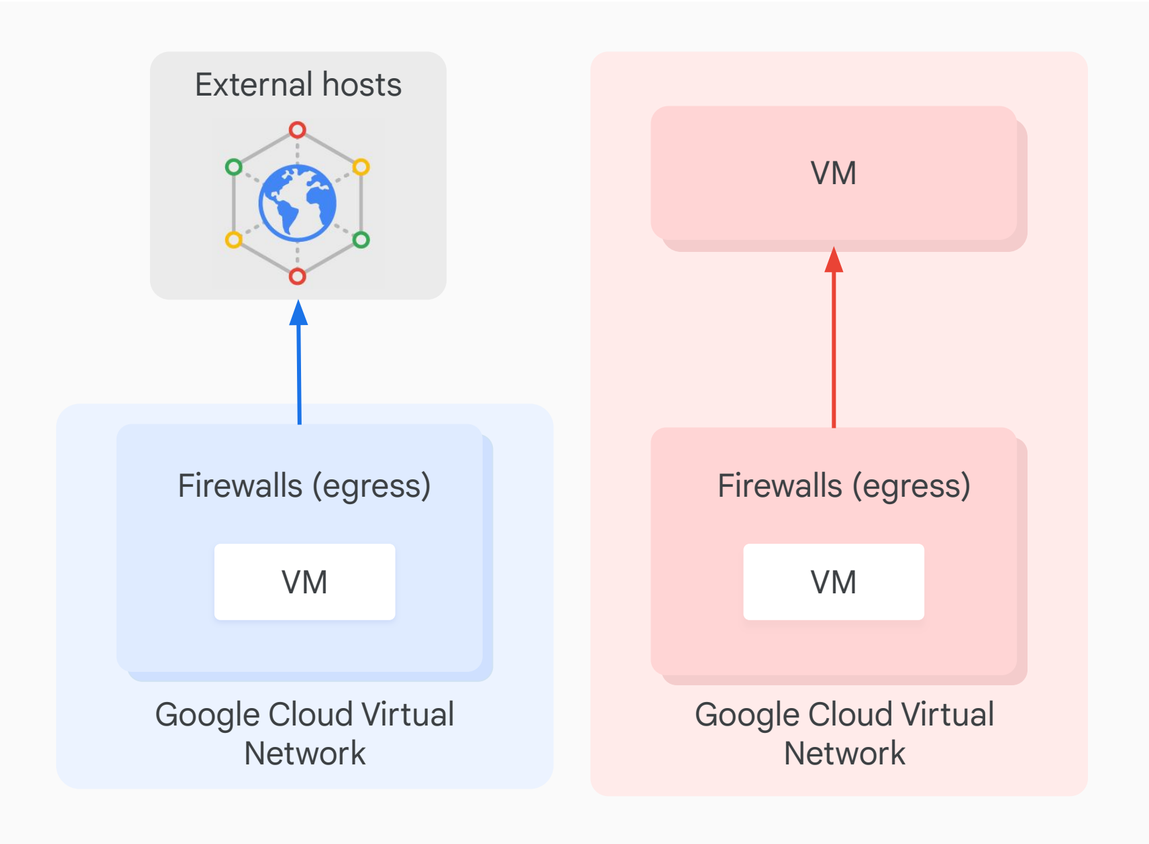


Cloud Firewall Rules

A firewall rule is composed of different parameters

Parameter	Details
`direction`	Inbound connections are matched against `ingress` rules only.
	Outbound connections are matched against `egress` rules only.
`source or destination`	For the `ingress` direction, `sources` can be specified as part of the rule with IP addresses, source tags or a source service account.
	For the `egress` direction, `destinations` can be specified as part of the rule with one or more ranges of IP addresses.
`protocol` **`and`** `port`	Any rule can be restricted to apply to specific protocols only or specific combinations of protocols and ports only.
`action`	To allow or deny packets that match the direction, protocol, port, and source or destination of the rule.
`priority`	Governs the order in which rules are evaluated; the first matching rule is applied.
`Rule assignment`	All rules are assigned to all instances, but you can assign certain rules to certain instances only.

Google Cloud firewall use case: Egress



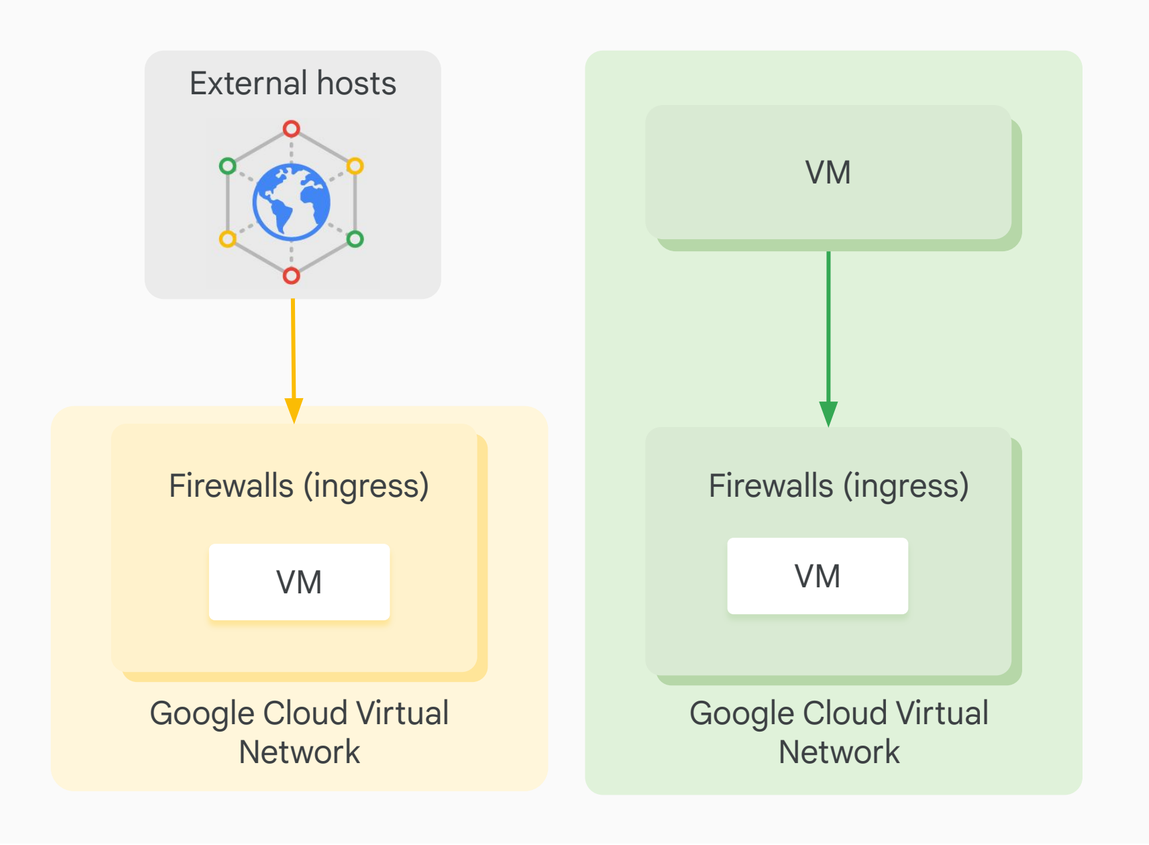
Conditions

- Destination CIDR ranges
- Protocols
- Ports

Action

- Allow: permit the matching egress connection
- Deny: block the matching egress connection

Google Cloud firewall use case: Ingress



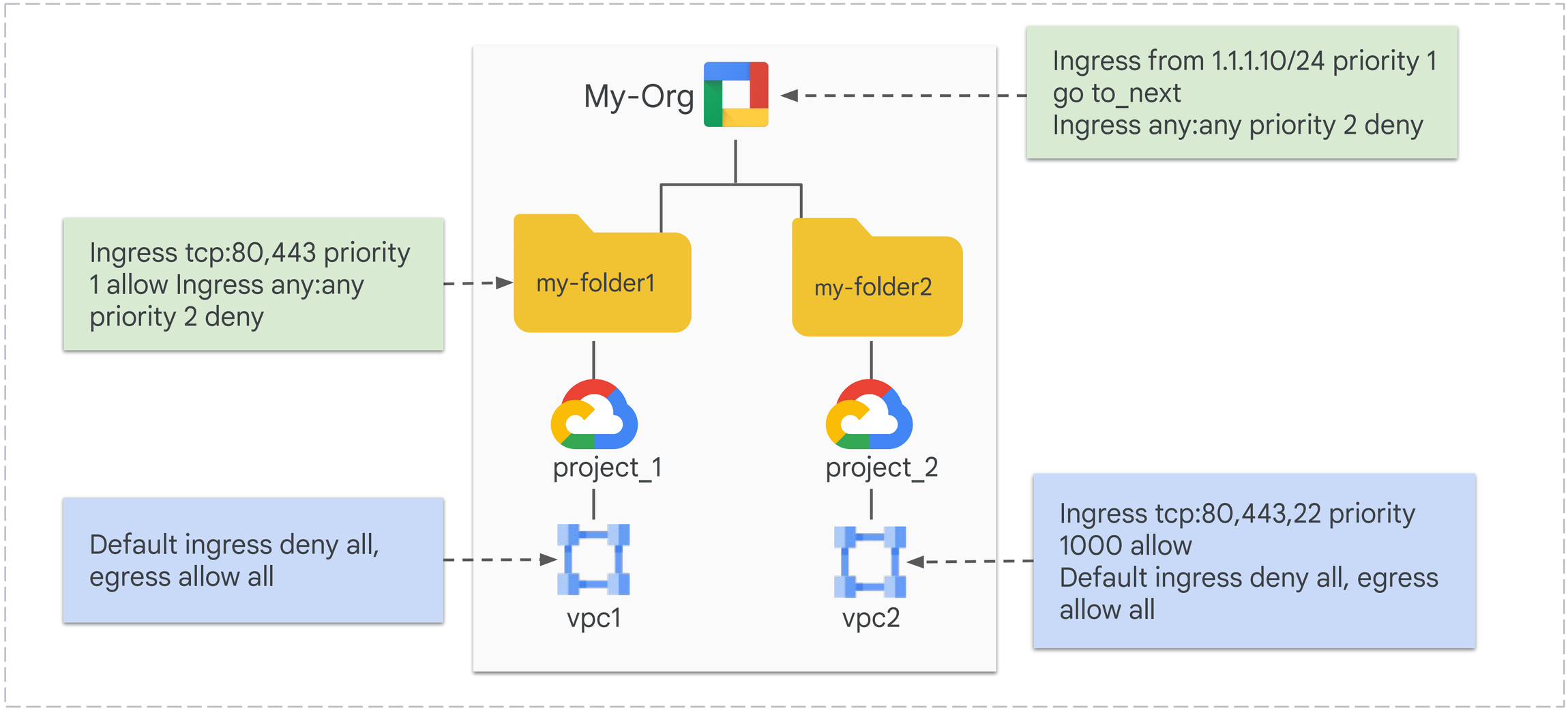
Conditions:

- Source CIDR ranges
- Protocols
- Ports

Action:

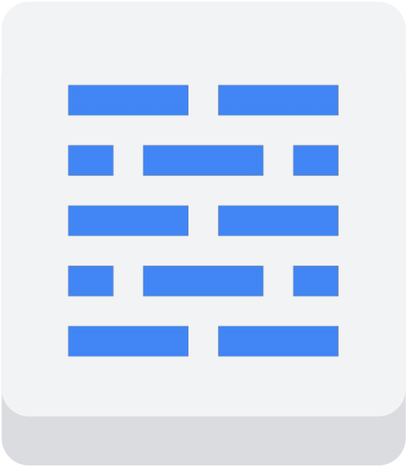
- Allow: permit the matching ingress connection
- Deny: block the matching ingress connection

Hierarchical firewall policies



Cloud Next Generation Firewall (NGFW)

- Distributed firewall service
- Supports network and firewall policies
- Supports VPC firewall rules
- Firewall rule logging
- IAM-governed tags for micro-segmentation
- Address groups allow combining multiple addresses/ranges into a single logical unit
- Three tiers: Essentials, Standard, and Enterprise



All features are available in all tiers

Cloud NGFW Standard

All of the features of NGFW Essentials, plus:

FQDN objects in firewall rules

Filter traffic by domain

Threat Intelligence for firewall rules

Allow/block traffic based on Threat Intelligence lists

Geolocation in firewall rules

Allow/block traffic based on geolocation

Cloud NGFW Enterprise

All of the features of NGFW Standard, plus:

- Advanced layer 7 capabilities
- Intrusion Prevention Service (in Preview as of 03/24)
- TLS interception and decryption

Tags for firewalls

Tags

- Used to define sources and targets in network firewall policies
- Not supported for VPC Firewall rules or hierarchical network policies
- Key:value format
- Sometimes referred to as secure tags
- NOT the same as network tags
- Subject to IAM controls (unlike network tags)

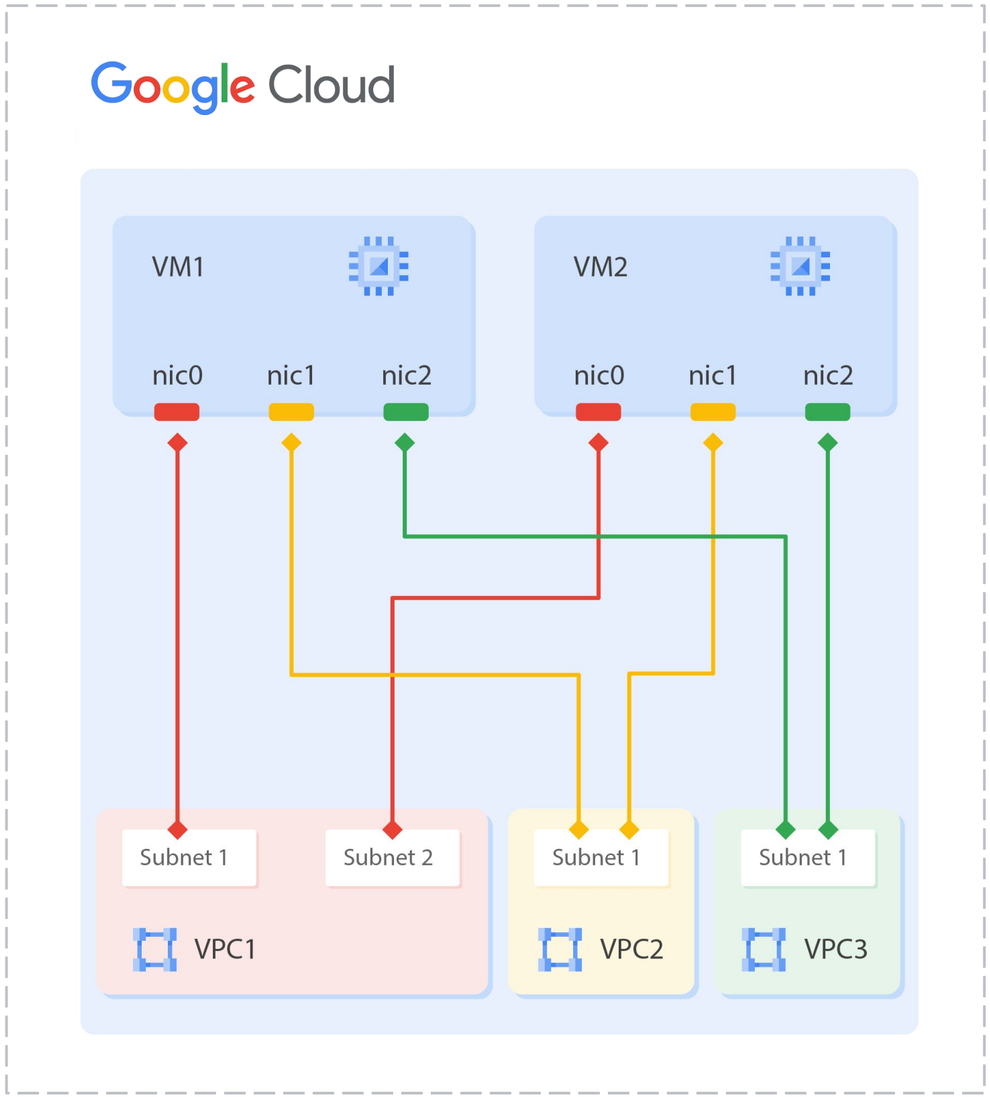
Multiple network interfaces

VPC networks are isolated (by default)

- Communicate within networks using **internal IP**
- Communicate across networks using **external IP**

Multiple Network Interfaces

- Network interface controllers (NICs)
- Each NIC is attached to a VPC network
- Communicate across networks using **internal IP**

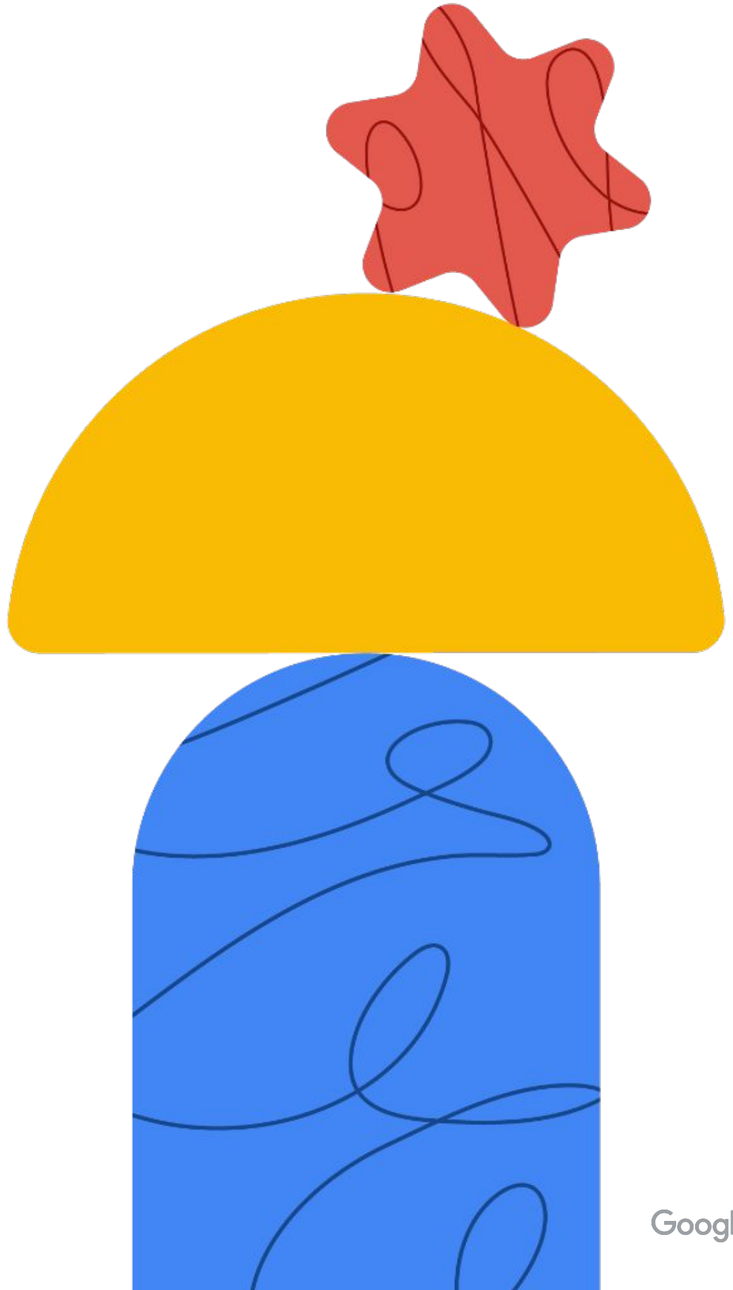


Multiple network interfaces limitations

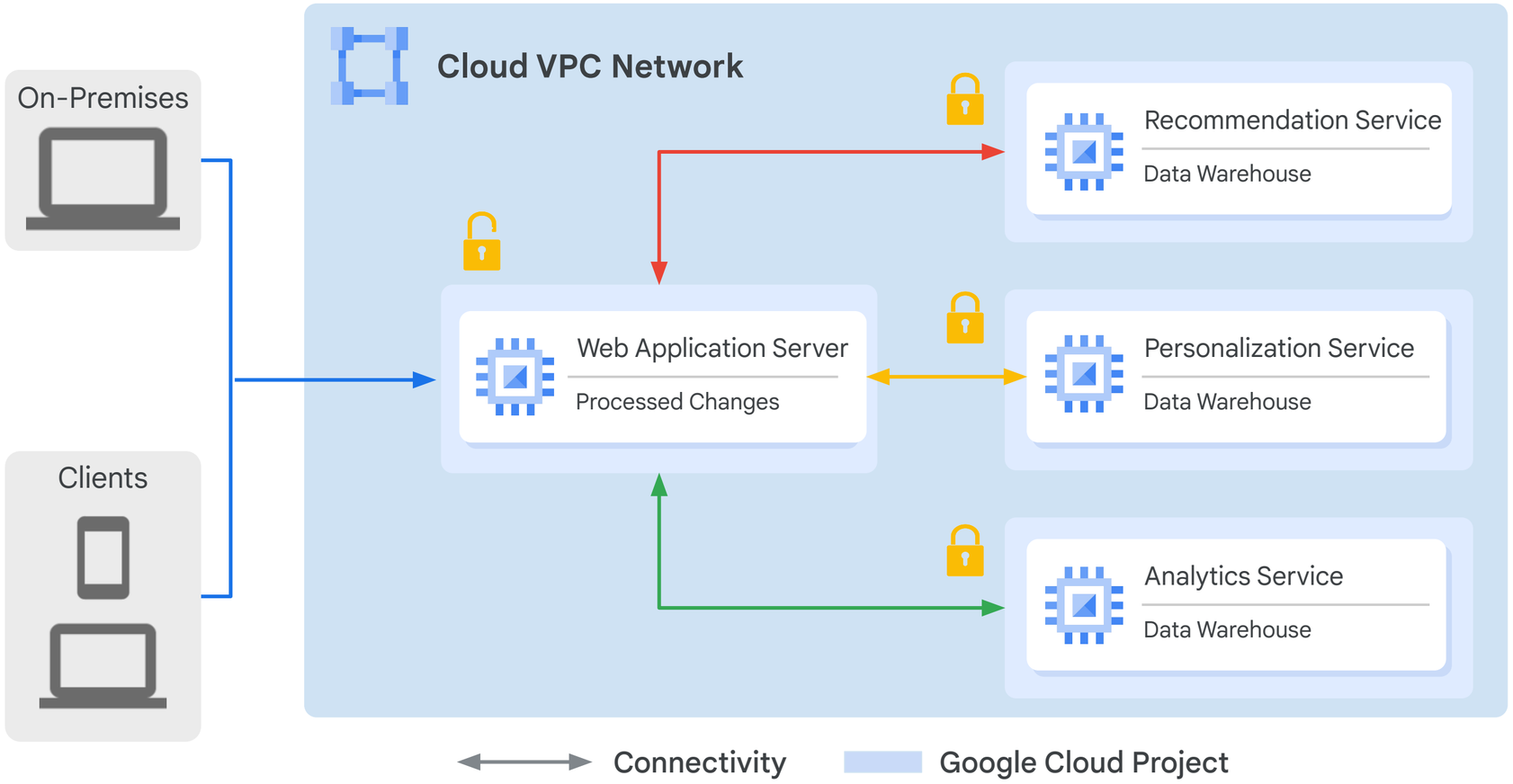
- Configure when you create instance
- Each interface in different network
- Networks' IP range cannot overlap
- Networks must exist to create VM
- Cannot delete interface without deleting VM
- Internal DNS only associated to nic0
- Up to 8 NICs, depends on VM

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

Sharing networks across projects



Shared VPC


On-Premises
Clients
Cloud VPC Network
Recommendation Service
Data Warehouse
Web Application Server
Processed Changes
Personalization Service
Data Warehouse
Analytics Service
Data Warehouse
Connectivity
Google Cloud Project

Provisioning shared VPC

Organization Admin

- Organization is the root node.
- Workplace or Cloud Identity super administrators assign Organization Admins.
- Nominates Shared VPC Admin (compute.xpnAdmin).

Provisioning shared VPC

Organization Admin

- Organization is the root node.
- Workplace or Cloud Identity super administrators assign Organization Admins.
- Nominates Shared VPC Admin (compute.xpnAdmin).

Shared VPC Admin

- Enables shared VPC for host project.
- Attaches service projects.
- Delegates access to some or all subnets in shared VPC network (compute.networkUser).

Provisioning shared VPC

Organization Admin

- Organization is the root node.
- Workplace or Cloud Identity super administrators assign Organization Admins.
- Nominates Shared VPC Admin (compute.xpnAdmin).

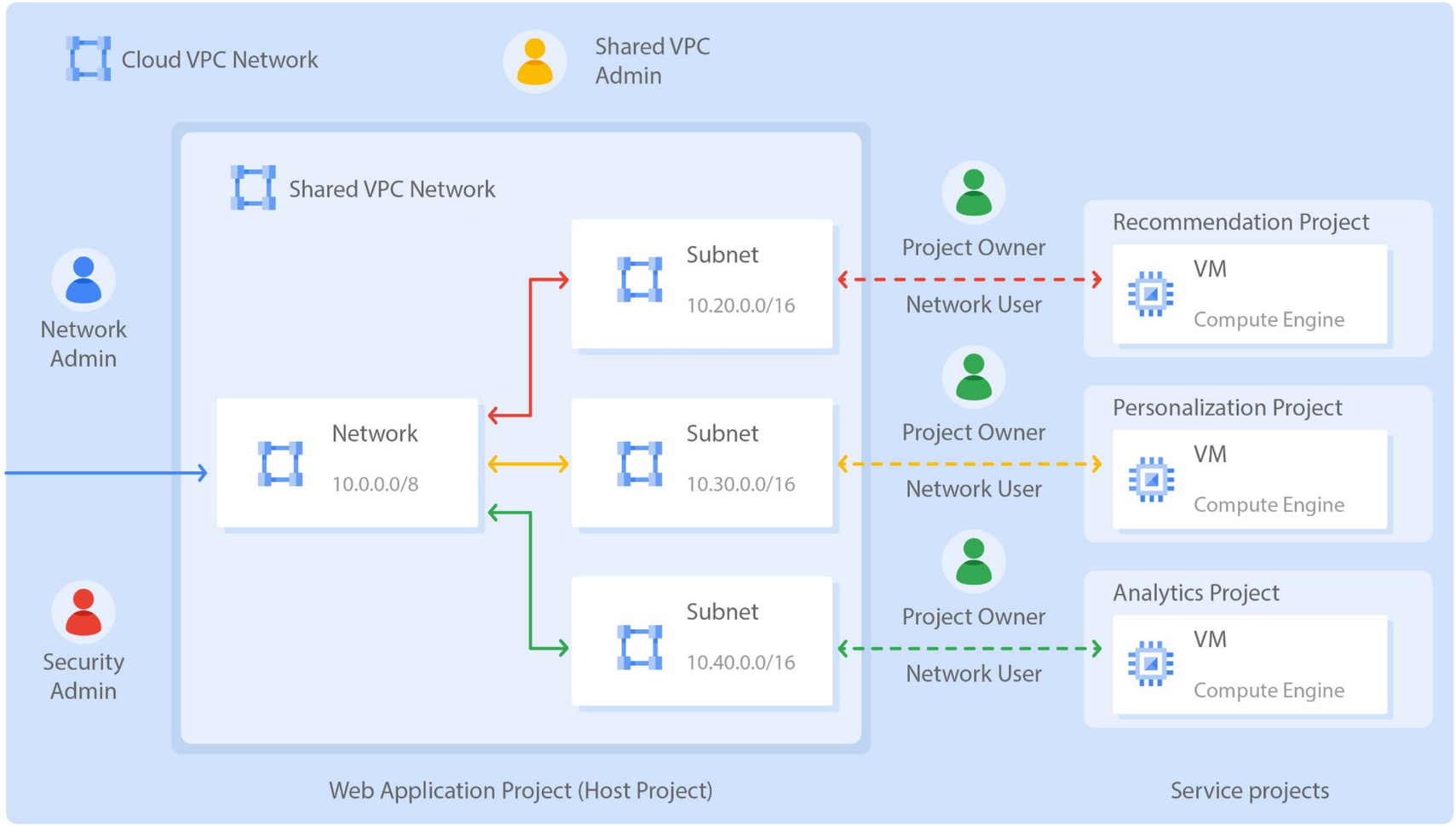
Shared VPC Admin

- Enables shared VPC for host project.
- Attaches service projects.
- Delegates access to some or all subnets in shared VPC network (compute.networkUser).

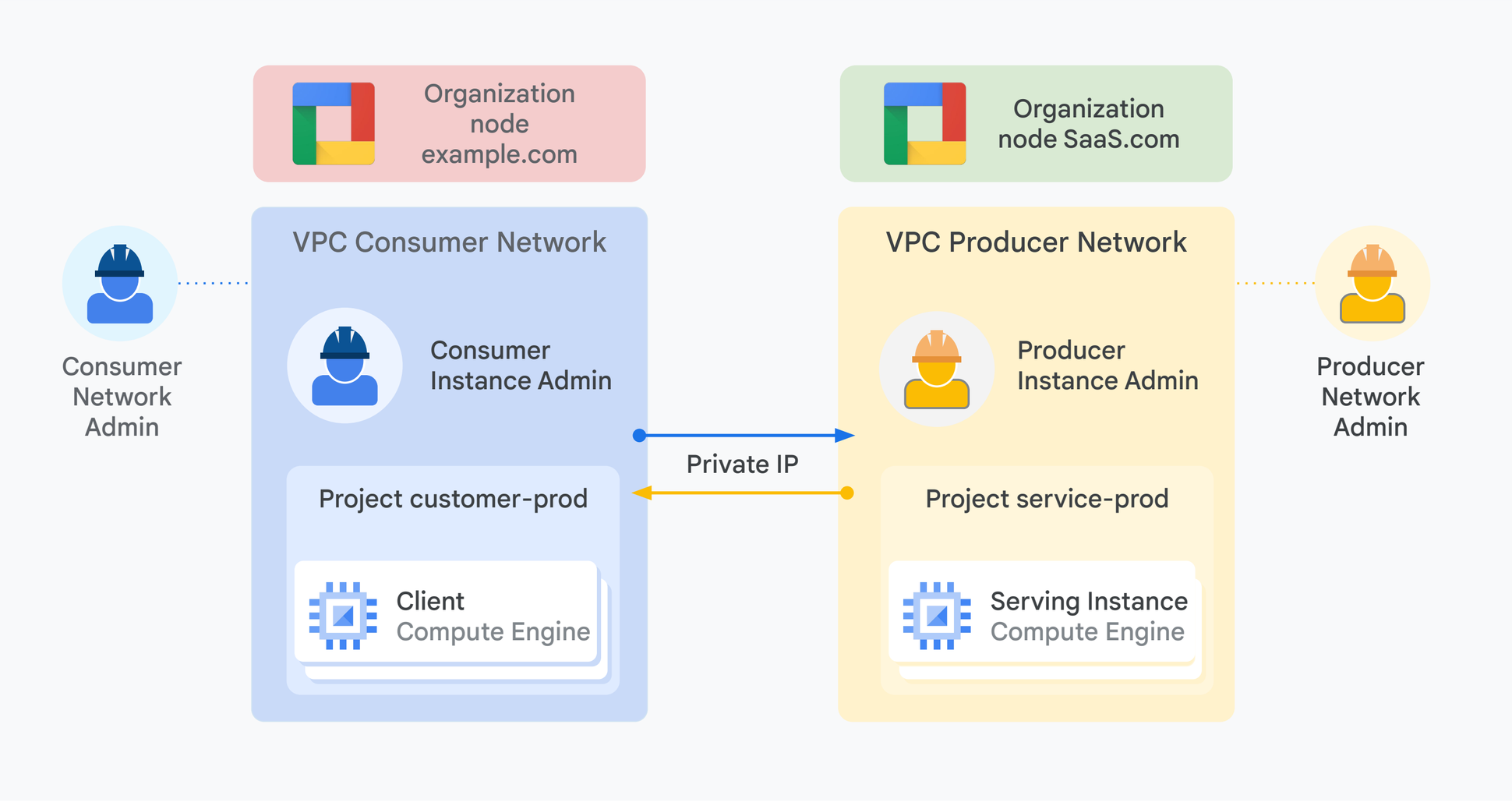
Service Project Admin

- Network User
- Control over service project resources:
  - Compute Instance Admin
  - Project Owner
- Create resources in shared VPC:
  - VM instances
  - Instance templates and groups
  - Static internal IP
  - Load balancers

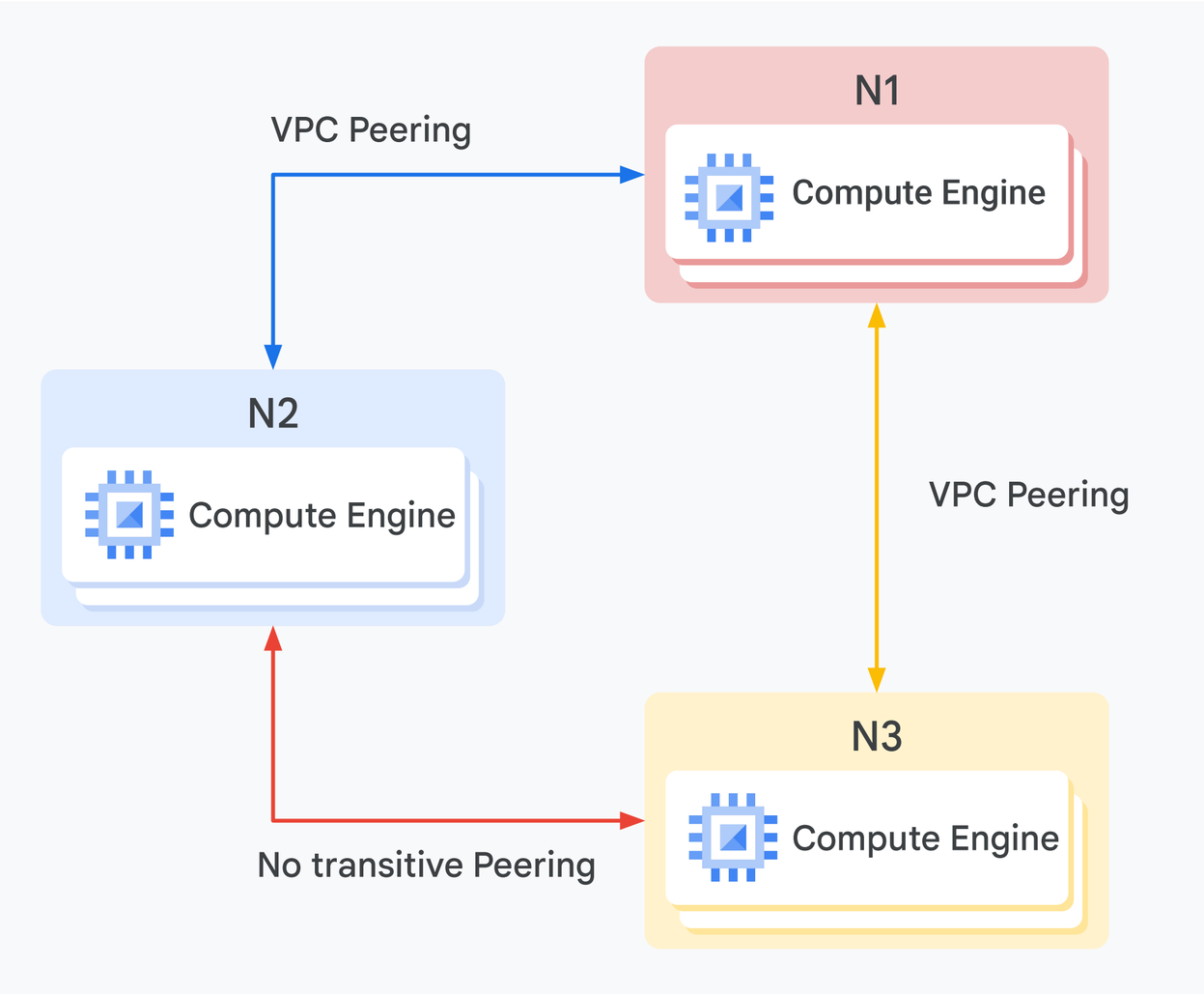
Shared VPC


Cloud VPC Network
Shared VPC Admin
Shared VPC Network
Network Admin
Network
10.0.0.0/8
Subnet
10.20.0.0/16
Subnet
10.30.0.0/16
Subnet
10.40.0.0/16
Security Admin
Project Owner
Network User
Project Owner
Network User
Project Owner
Network User
Recommendation Project
VM
Compute Engine
Personalization Project
VM
Compute Engine
Analytics Project
VM
Compute Engine
Web Application Project (Host Project)
Service projects

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

Remember when using VPC peering



Shared VPC vs. VPC peering

Consideration	Shared VPC	VPC Network Peering
Across Organizations	No	Yes
Within Project	No	Yes
Network Administration	Centralized	Decentralized

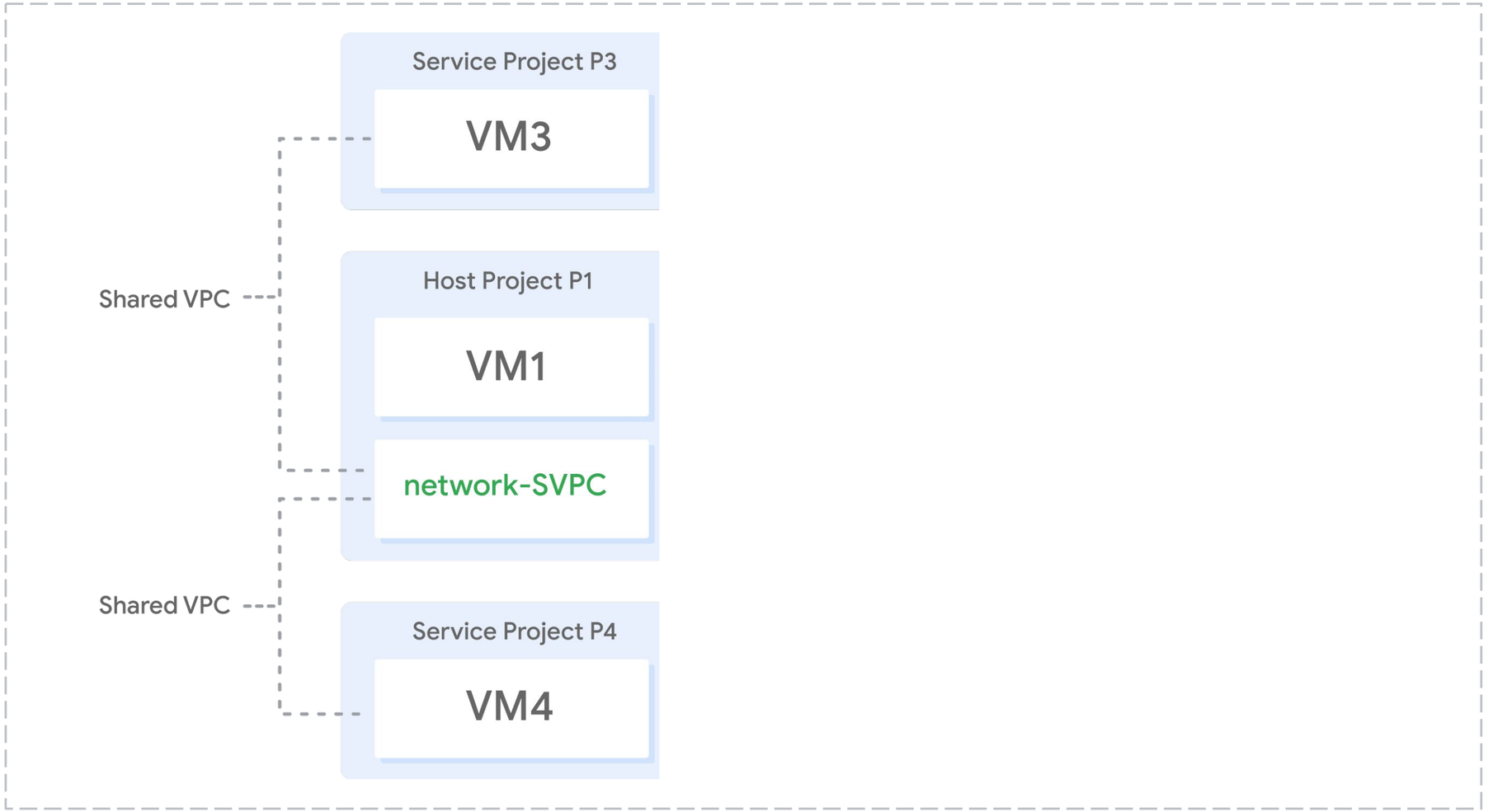
Shared VPC vs. VPC peering

Consideration	Shared VPC	VPC Network Peering
Across Organizations	No	Yes
Within Project	No	Yes
Network Administration	Centralized	Decentralized

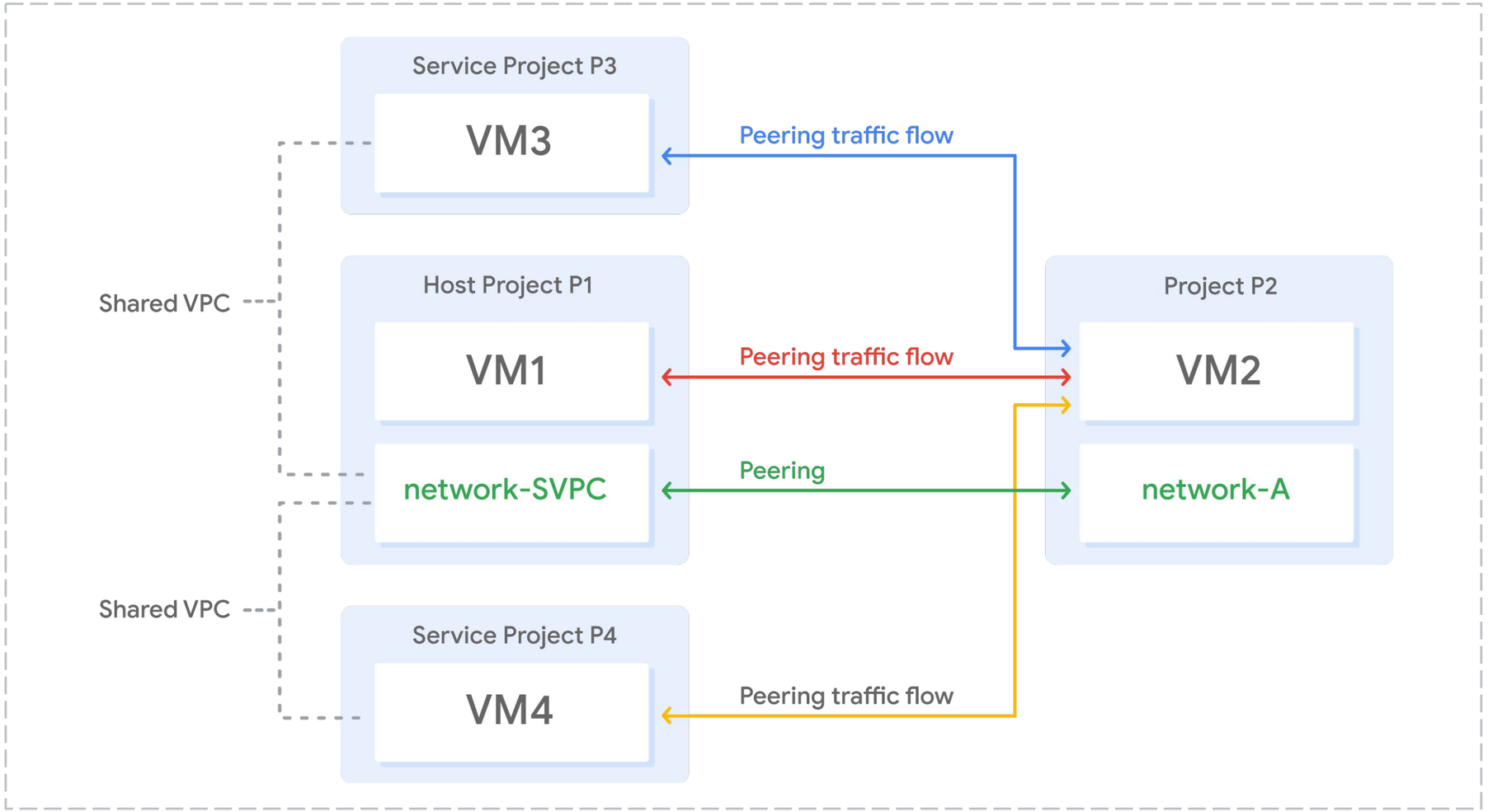
Organization Admin		
Shared VPC Admin		
Security and Network Admins		
Project Owner	Project Owner	Project Owner

Organization Admin (if same org)		
Security and Network Admins	Security and Network Admins	Security and Network Admins
Project Owner	Project Owner	Project Owner

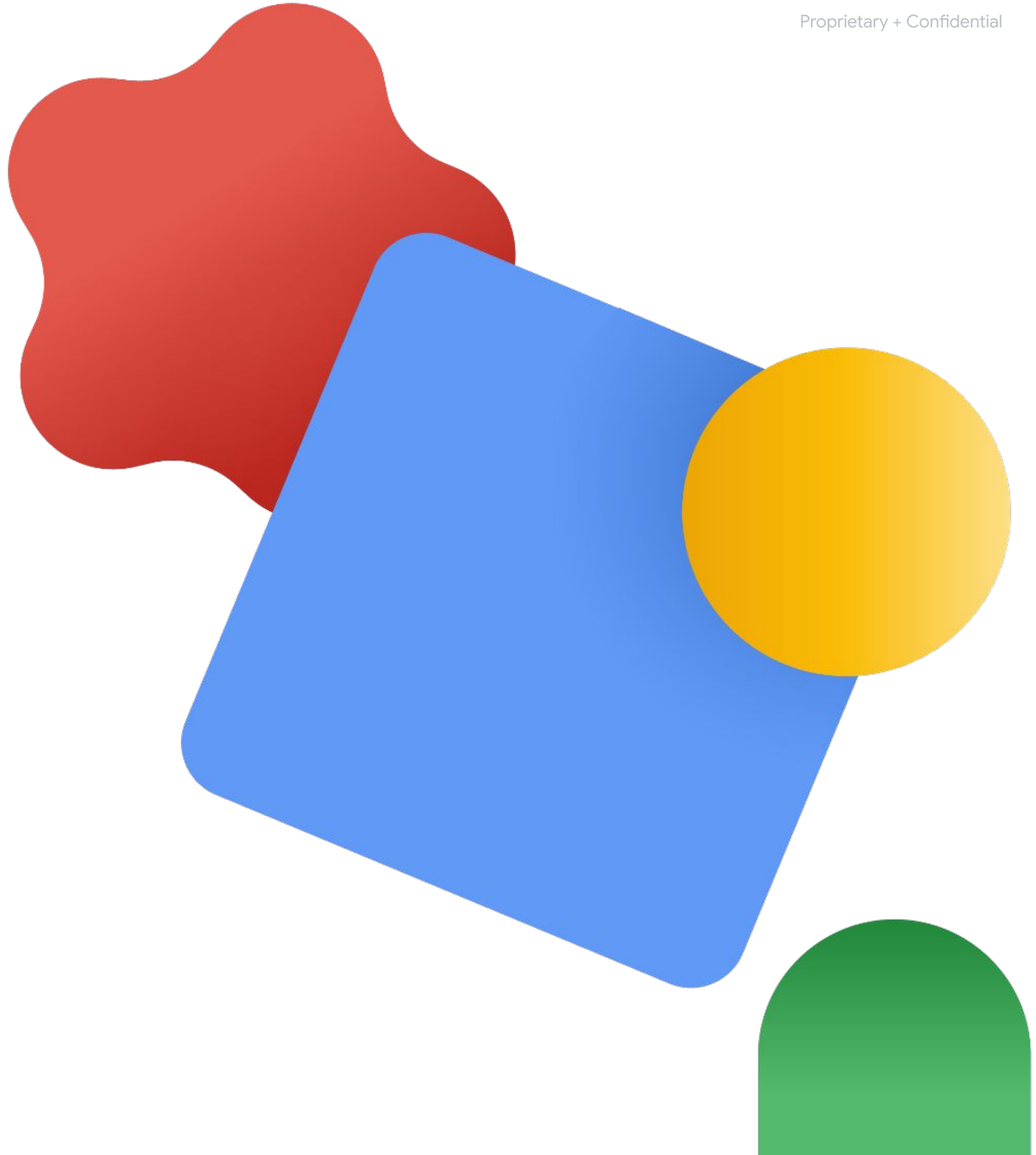
Peering with a shared VPC



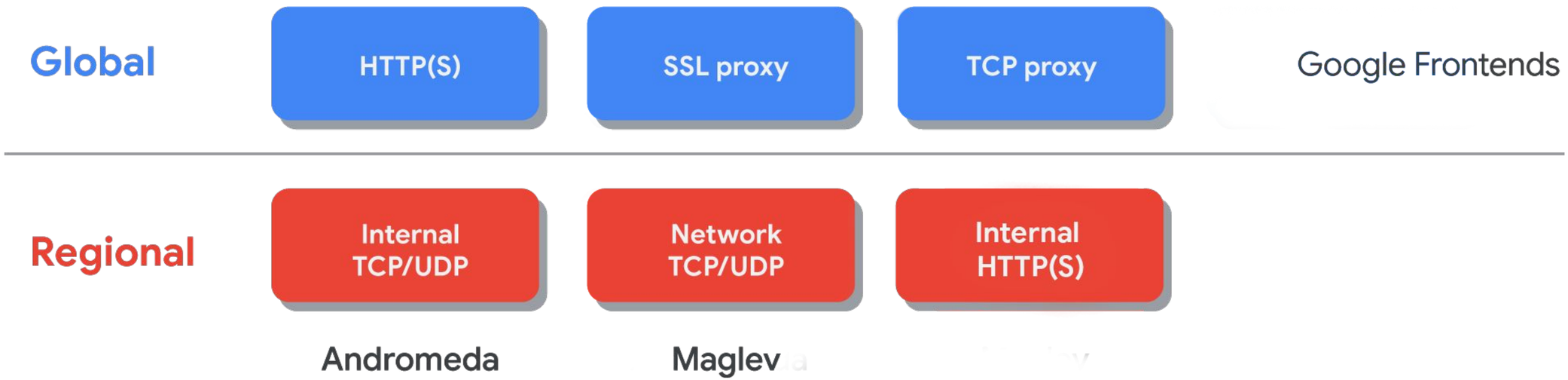
Peering with a shared VPC



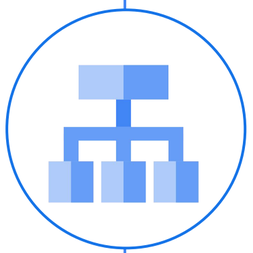
Load balancing



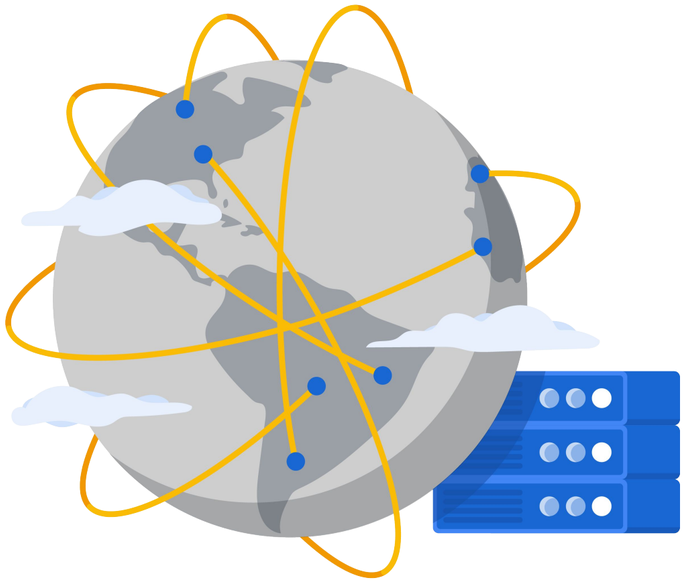
Global and regional load balancers



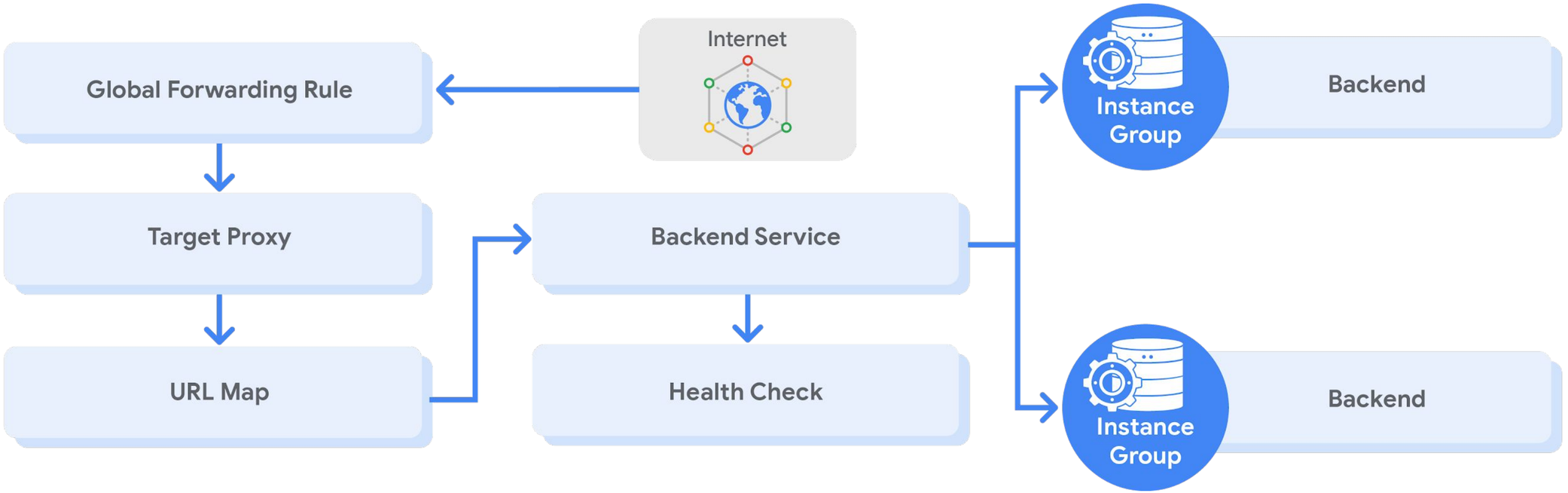
HTTP(S) load balancing



- Anycast IP address
- HTTP on port 80 or 8080
- HTTPs on port 443
- IPv4 or IPv6 clients
- Autoscaling
- URL maps

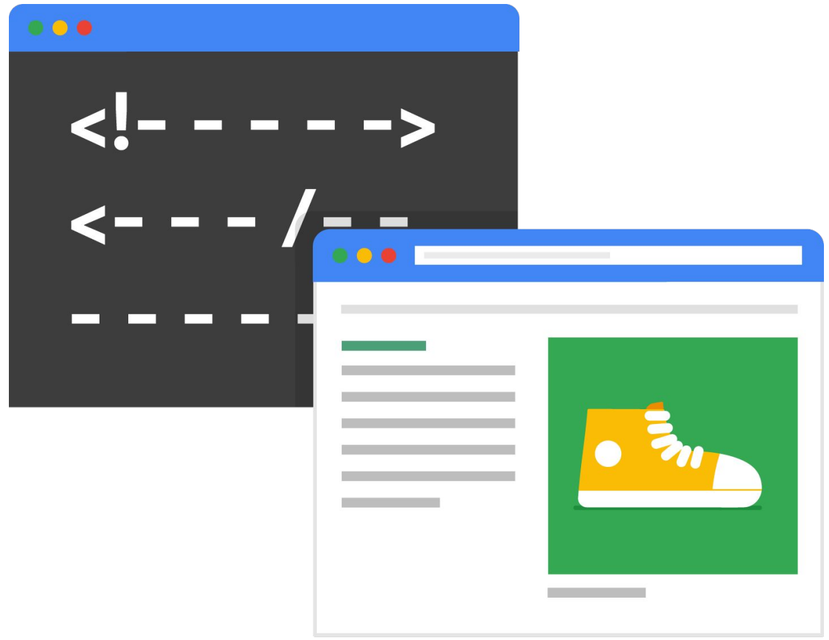


Architecture of an HTTP(S) load balancer



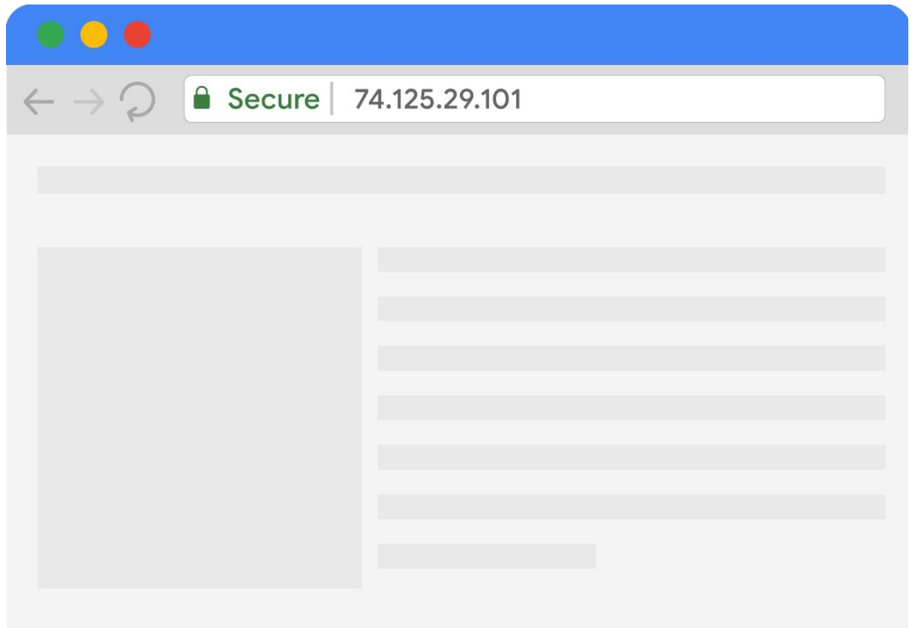
Backend services

- Health check
- Session affinity (optional)
- Timeout setting (30-sec default)
- One or more backends
  - An instance group (managed or unmanaged)
  - A balancing mode (CPU utilization or RPS)
  - A capacity scaler (ceiling % of CPU/Rate targets)



HTTP(S) load balancing

- Target HTTP(S) proxy
- One signed SSL certificate installed (at least)
- Client SSL session terminates at the load balancer
- Support the QUIC transport layer protocol



SSL certificates

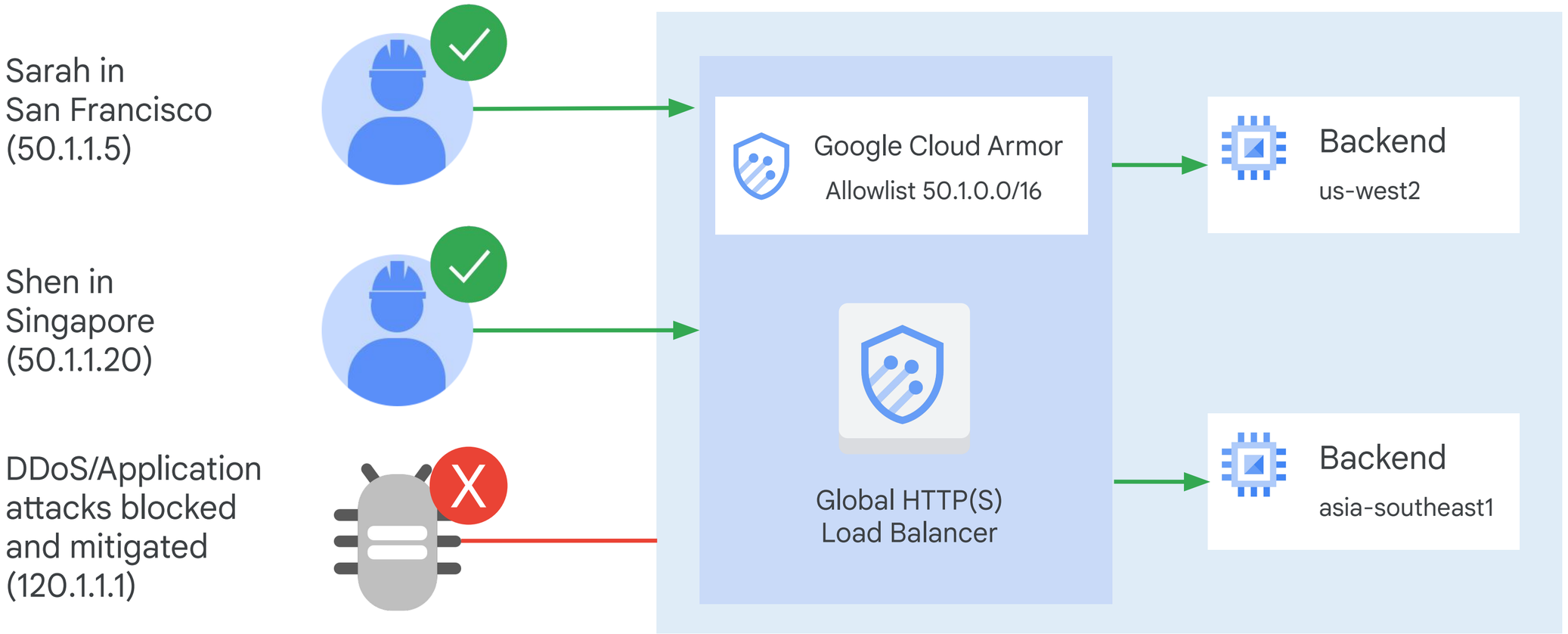
Required for HTTP(S) load balancing

Up to 10 SSL certificates (per target proxy)

Create an SSL certificate resource

Google Cloud Armor

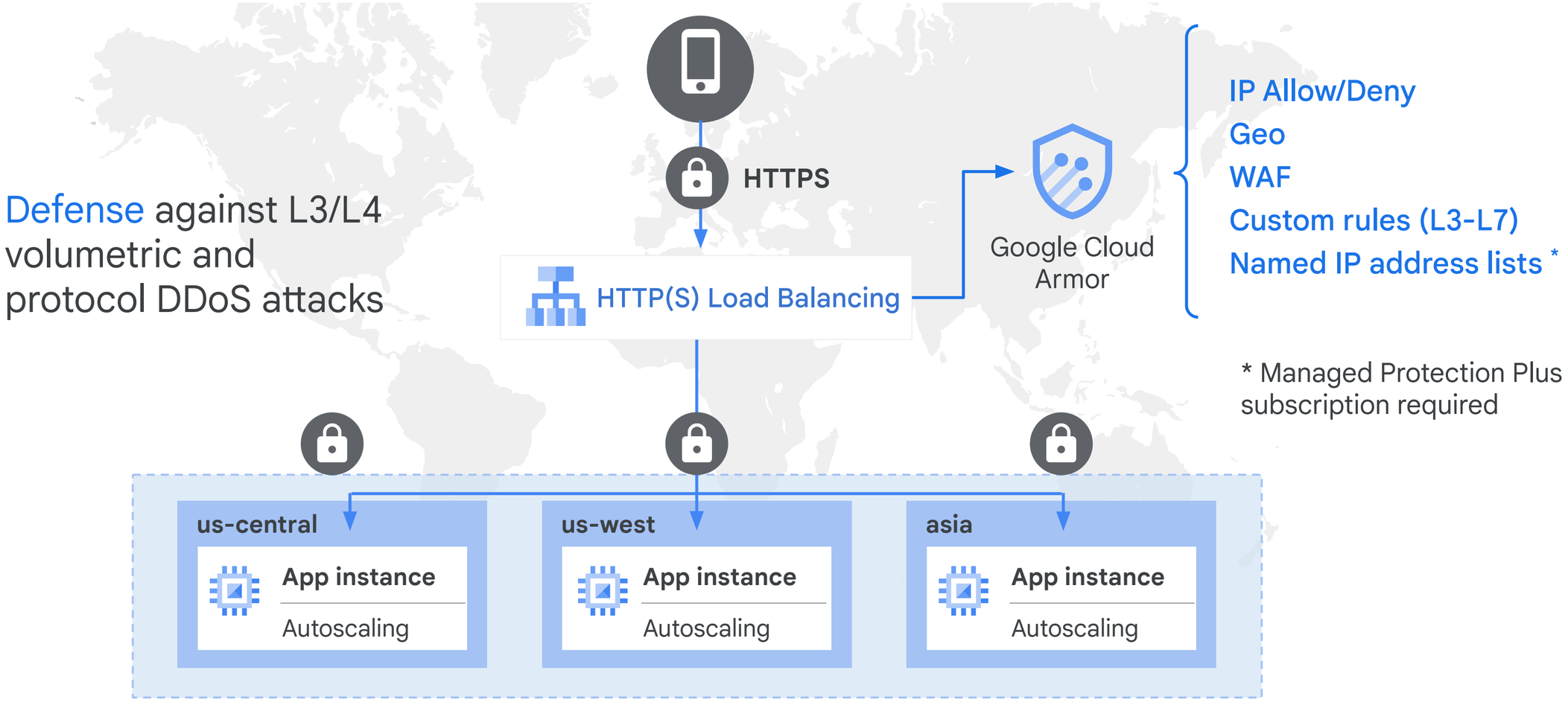
Works with HTTP(S) load balancing



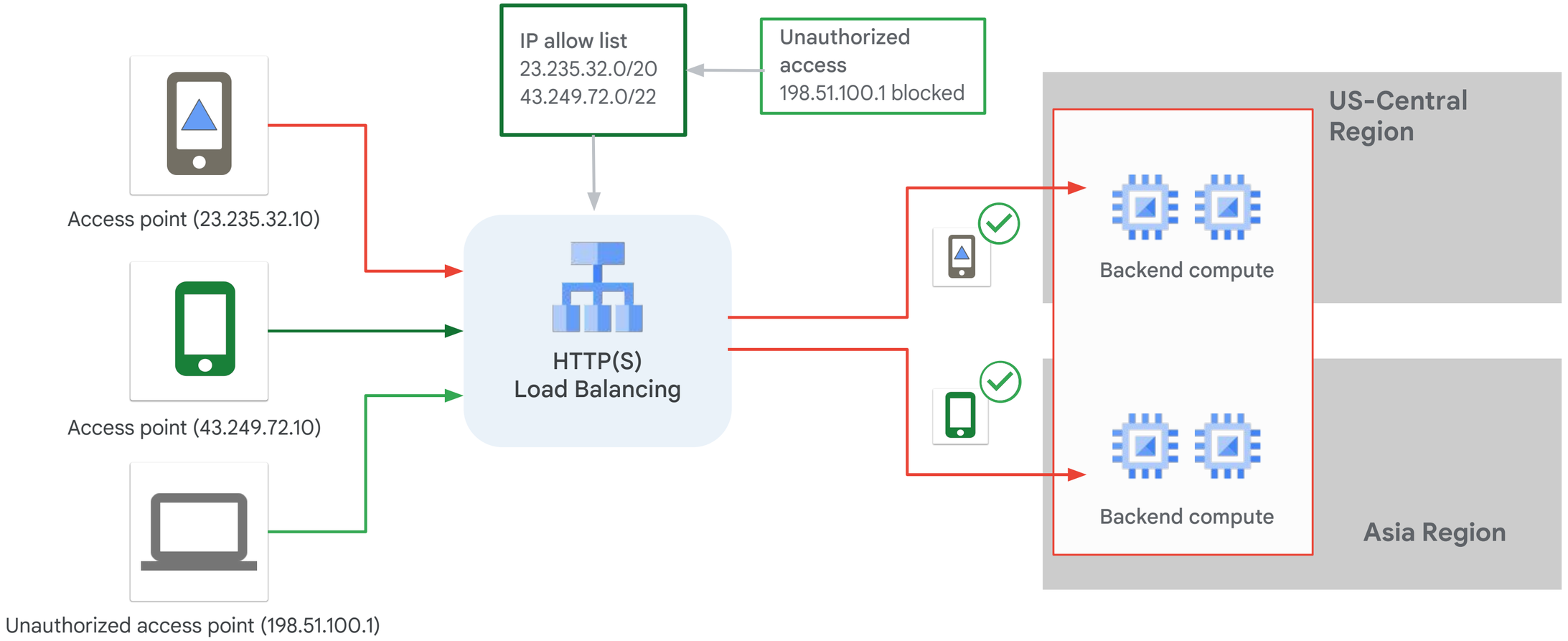
Security policies with deny and allow rules

Denying	Allowing	IPv4 and IPv6	Deny rule	Priority
Blocks source IP address or CIDR range from accessing HTTP(S) load balancers.	Allows a source IP address or CIDR range to access HTTP(S) load balancers.	IPv4 and IPv6 addresses are supported in allow and deny rules.	Configure the deny rule to display a 403, 404, or 502 error code.	Designate the order in which multiple rules are evaluated by assigning a priority.

Google Cloud Armor Web Application Firewall



Google Cloud Armor named IP address lists



Google Cloud Armor Managed Protection Plus

	Google Cloud Armor Standard	Managed Protection Plus
Billing method	Pay-as-you-go	Monthly subscription + Data Processing Fee
DDoS attack protection	• HTTP(S) Load Balancing • TCP Proxy Load Balancing • SSL Proxy Load Balancing	• HTTP(S) Load Balancing • TCP Proxy Load Balancing • SSL Proxy Load Balancing
Google Cloud Armor WAF	Per policy, per rule, per request	Included with Plus subscription
Resource limits	Up to quota limit	Up to quota limit
Preconfigured WAF rules	Yes	Yes
Time commitment	N/A	One year
Named IP address lists	No	Yes
Adaptive Protection	Alerting only	Yes
DDoS response support	N/A	Yes (w/ Premium Support)
DDoS bill protection	N/A	Yes

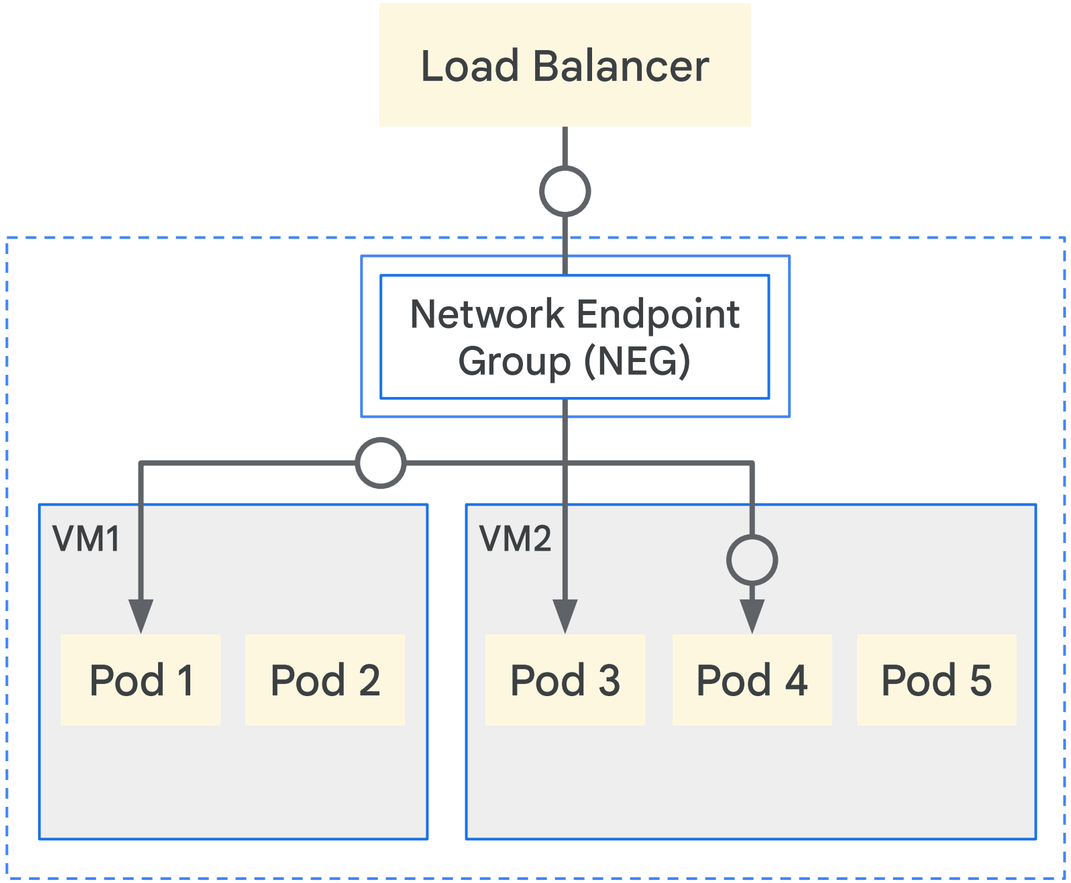
Google Cloud Armor

Integrates with the Security Command Center

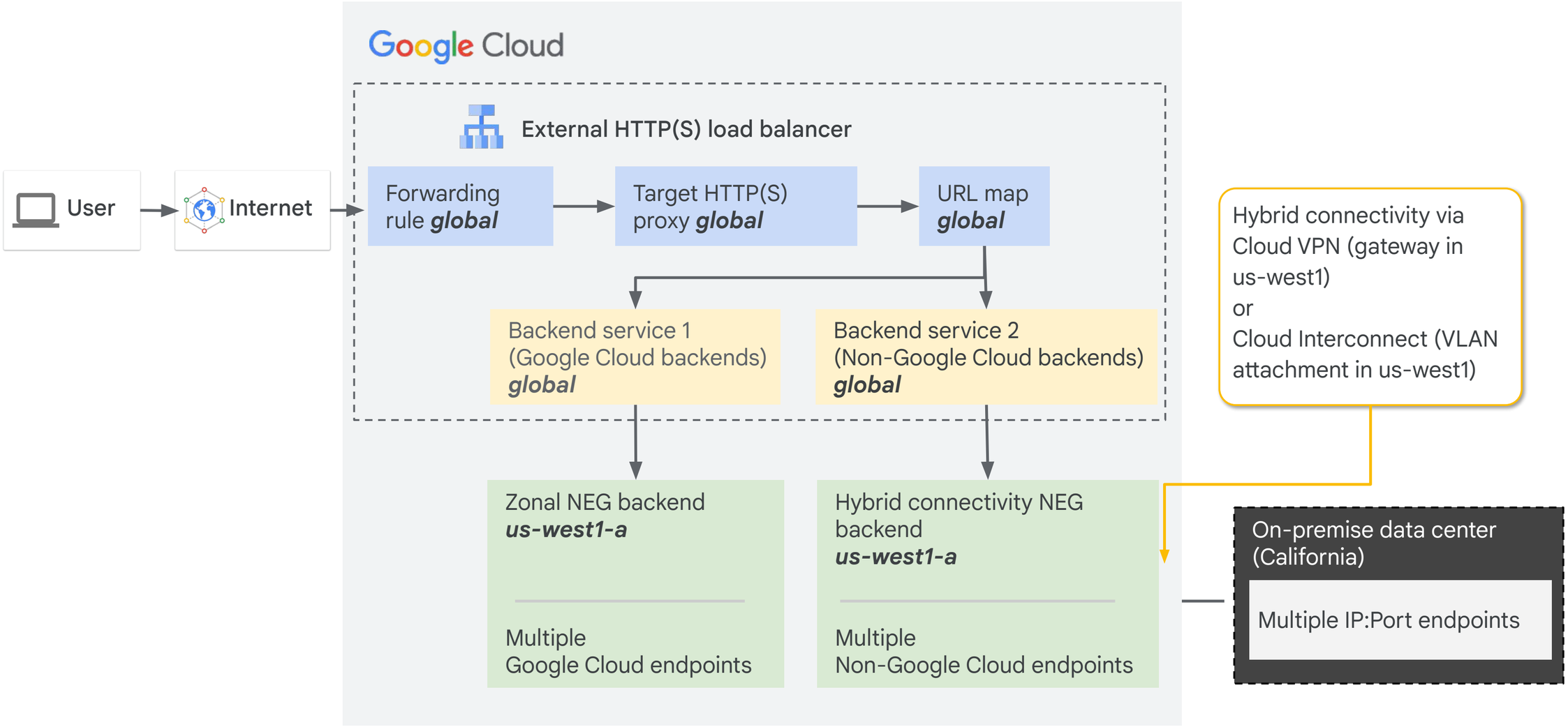
- Alerts users of potential Layer 7 attacks.
- Findings automatically sent to Security Command Center.
- Organizations with Security Command Center enabled and Google Cloud Armor receive real-time notifications of two events:
  - Allowed Traffic Spike
  - Increasing Deny Ratio

Network endpoint groups

- Specifies a group of backend endpoints or services
- Used as a backend for certain load balancers
- Zonal, internet and serverless endpoint types

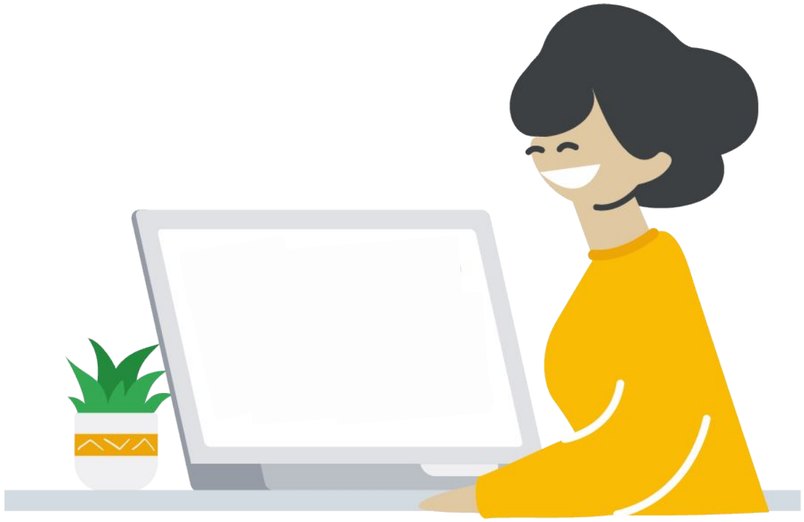


Hybrid load balancing for External HTTP(S) load balancing



SSL proxy load balancing

- Global load balancing for encrypted, non-HTTP traffic
- Terminates SSL sessions at load balancing layer
- IPv4 or IPv6 clients



SSL proxy load balancing

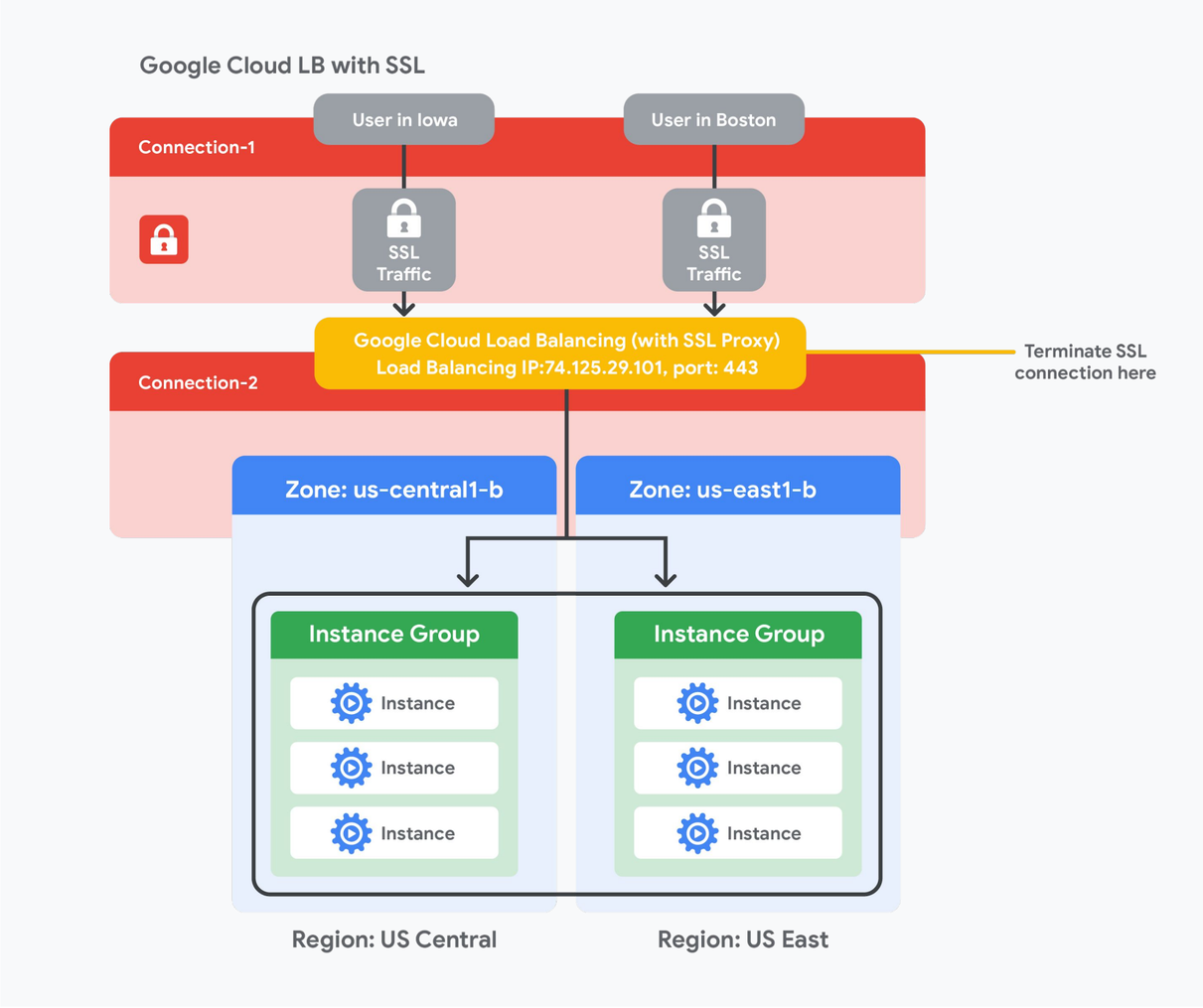
01 Intelligent routing

02 Certificate management

03 Security patching

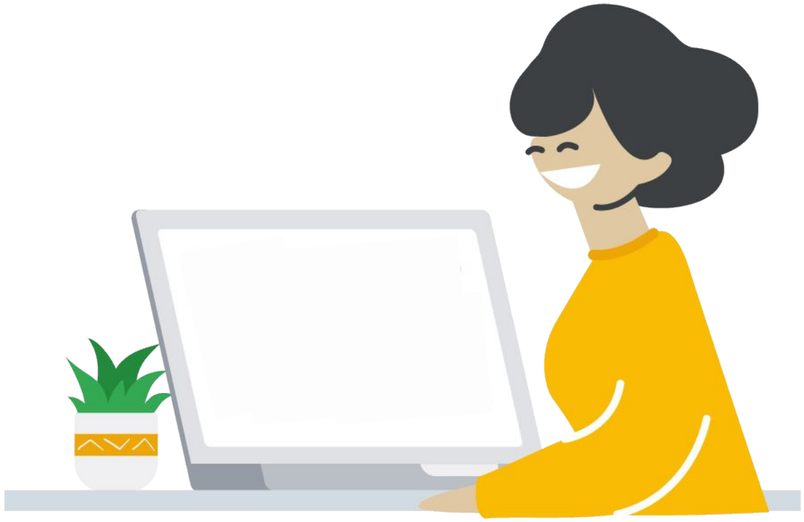
04 SSL policies

Example: SSL proxy load balancing



TCP proxy load balancing

- Global load balancing for unencrypted, non-HTTP traffic
- Terminates TCP sessions at load balancing layer
- IPv4 or IPv6 clients

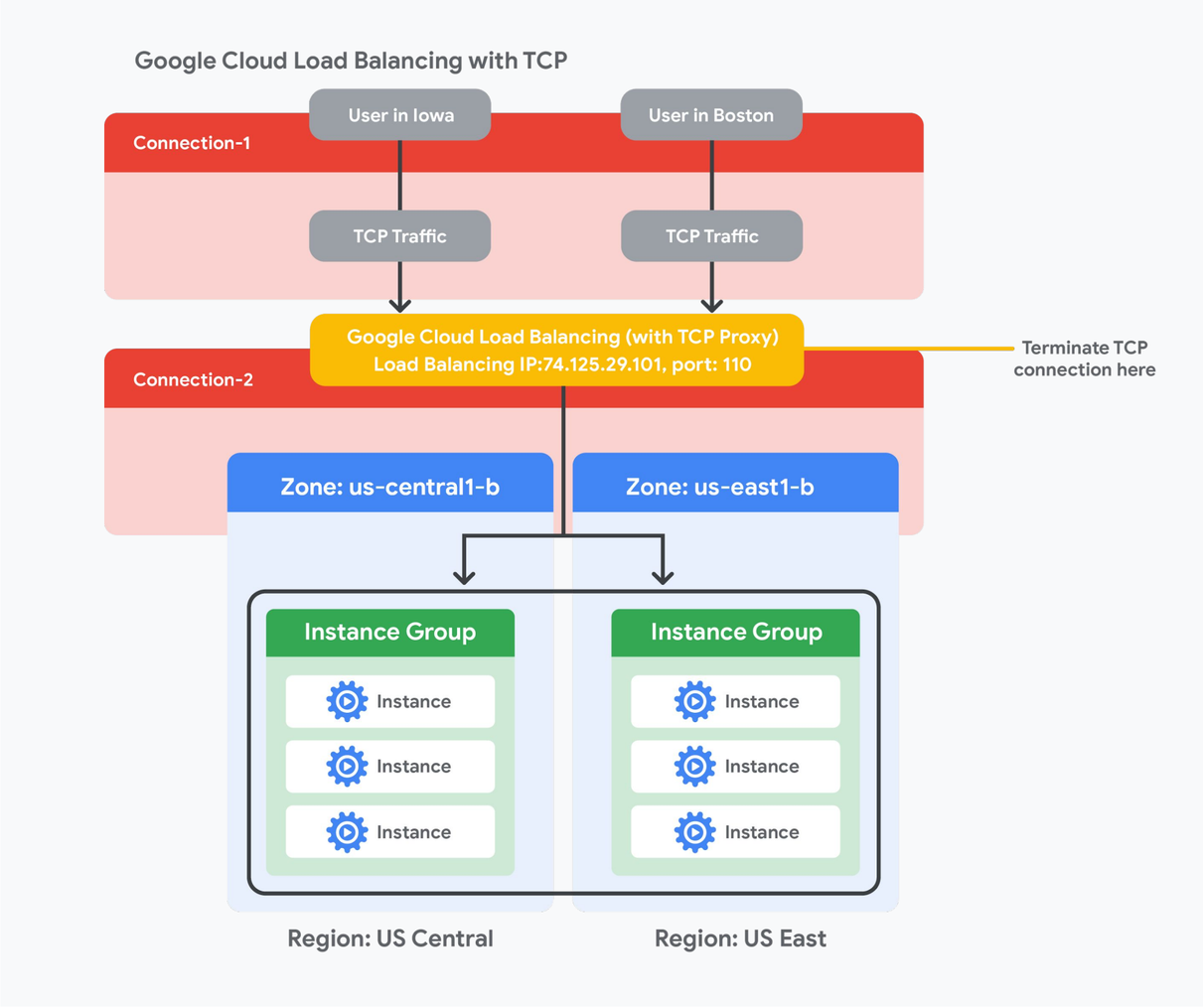


TCP proxy load balancing

01 Intelligent routing

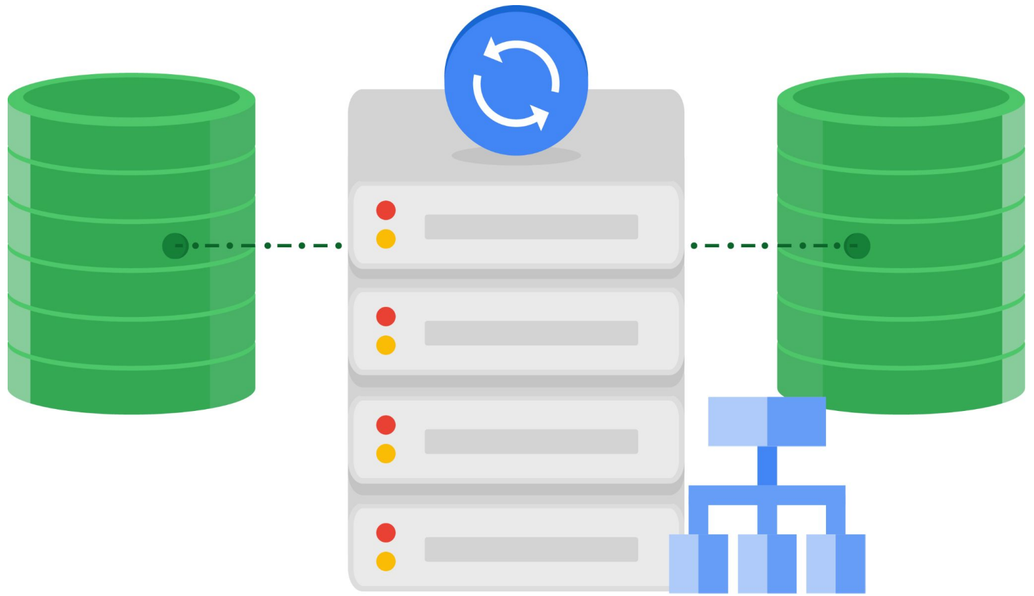
02 Security patching

Example: TCP proxy load balancing



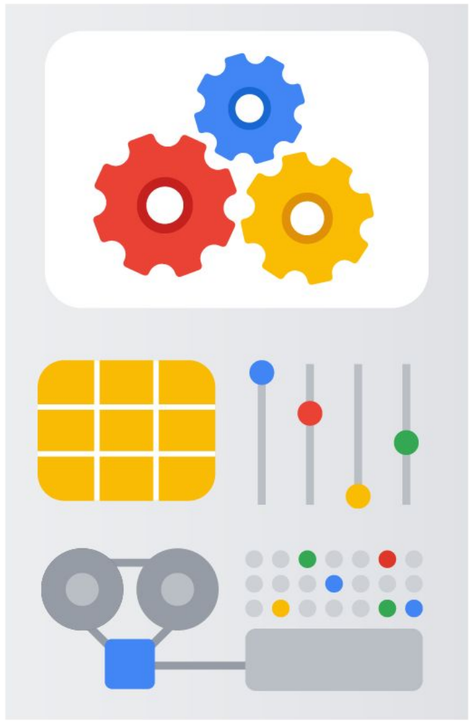
Network load balancing

- Regional, *non-proxied* load balancer
- Forwarding rules (IP protocol data)
- Traffic:
  - UDP
  - TCP/SSL ports
- Backends:
  - Instance group
  - Target pool

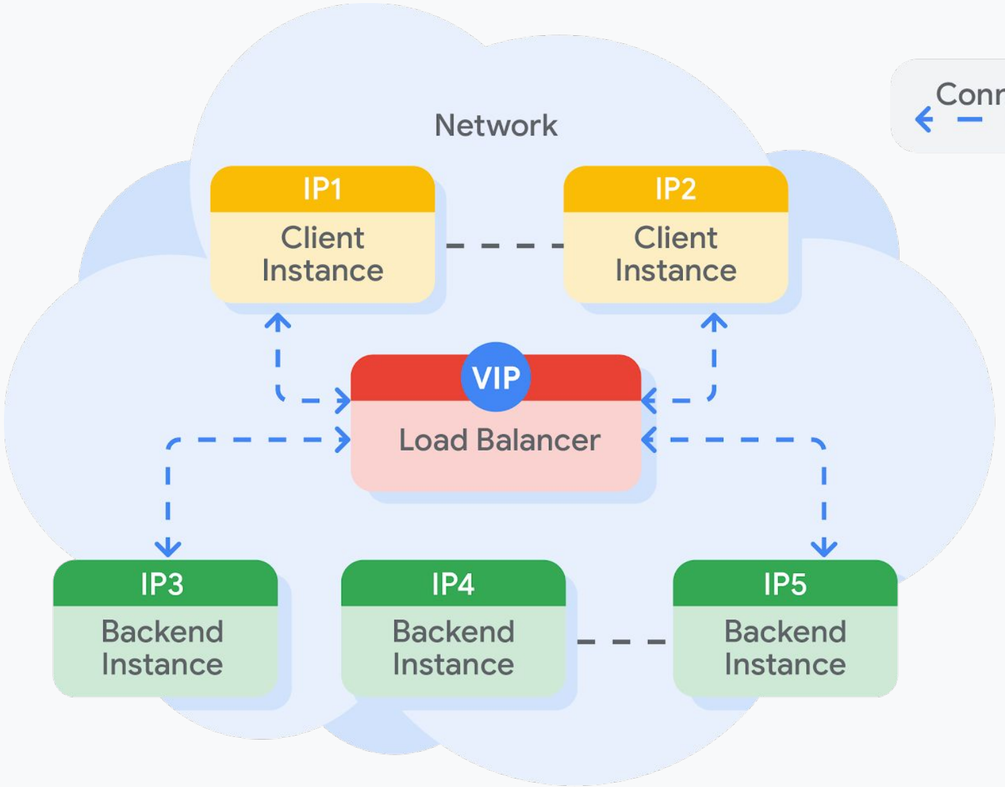


Internal TCP/UDP load balancing

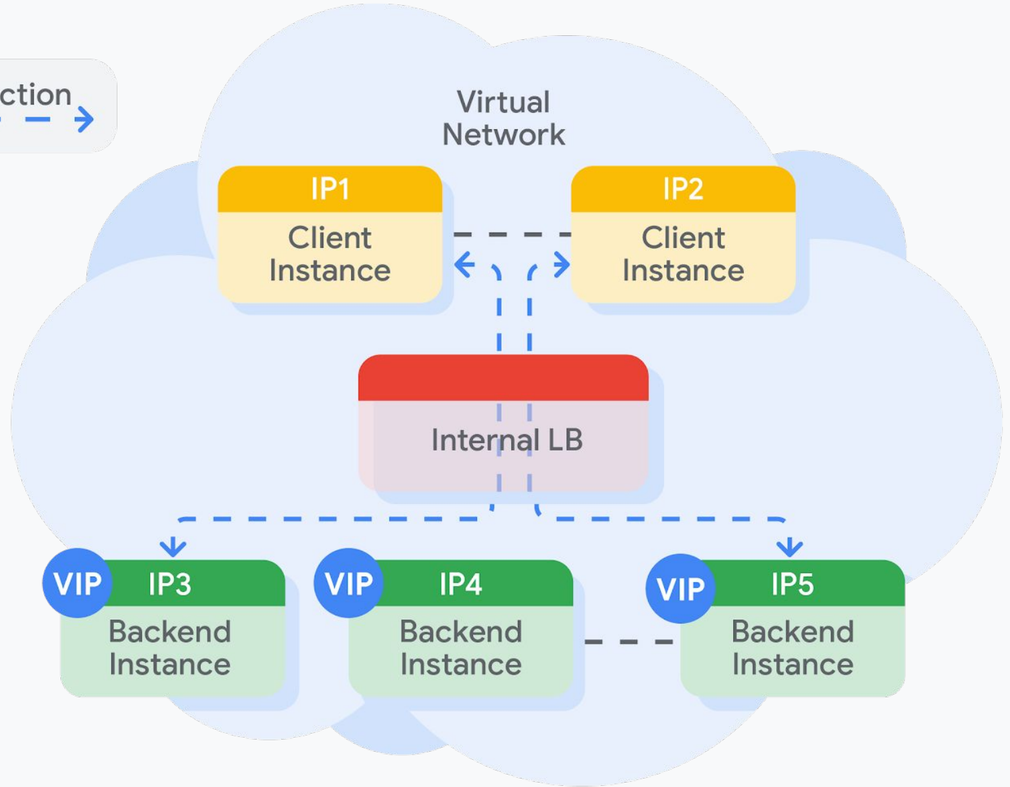
- Regional load balancer
  - VM instances in same region
- TCP/UDP traffic
- Reduced latency, simpler configuration
- Software-defined, fully distributed load balancing
- Global access option



Software-defined, fully distributed load balancing



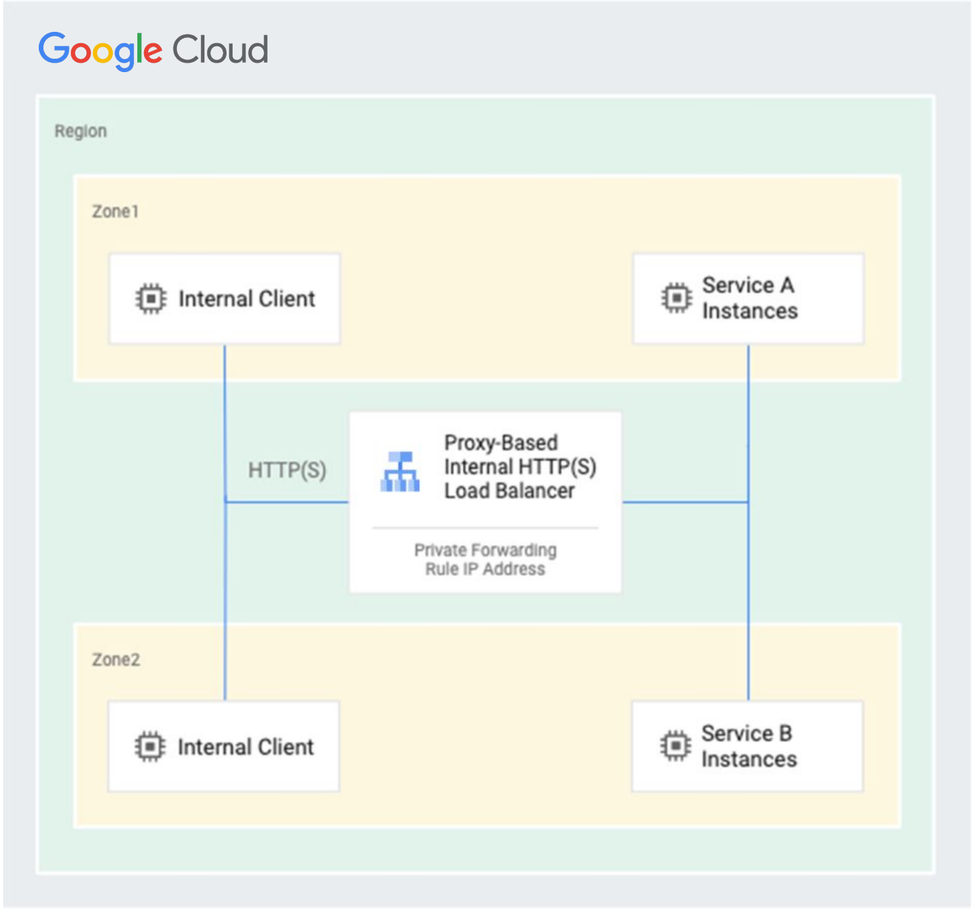
Traditional proxy model of internal load balancing



Internal TCP/UDP load balancer

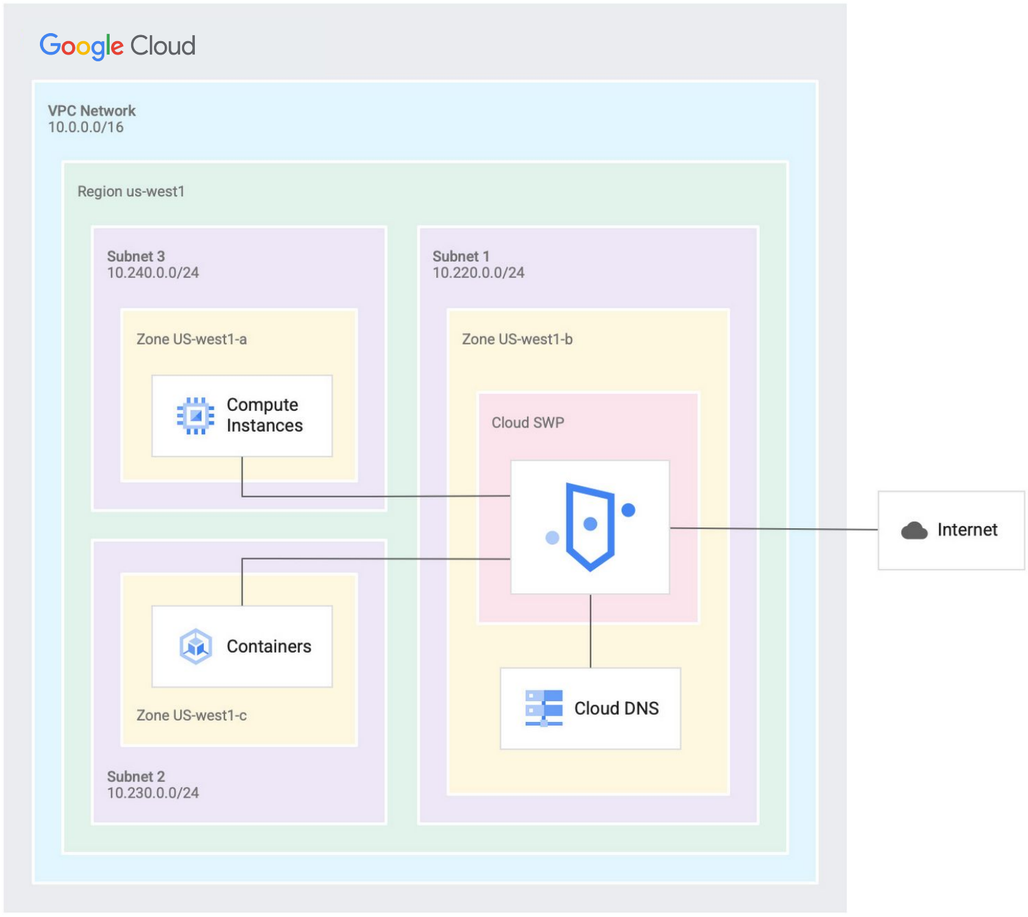
Internal HTTP(S) load balancing

- Regional, private load balancing
  - VM instances in same region
  - RFC 1918 IP addresses
- HTTP, HTTPS, or HTTP/2 protocols
- Based on open source Envoy proxy

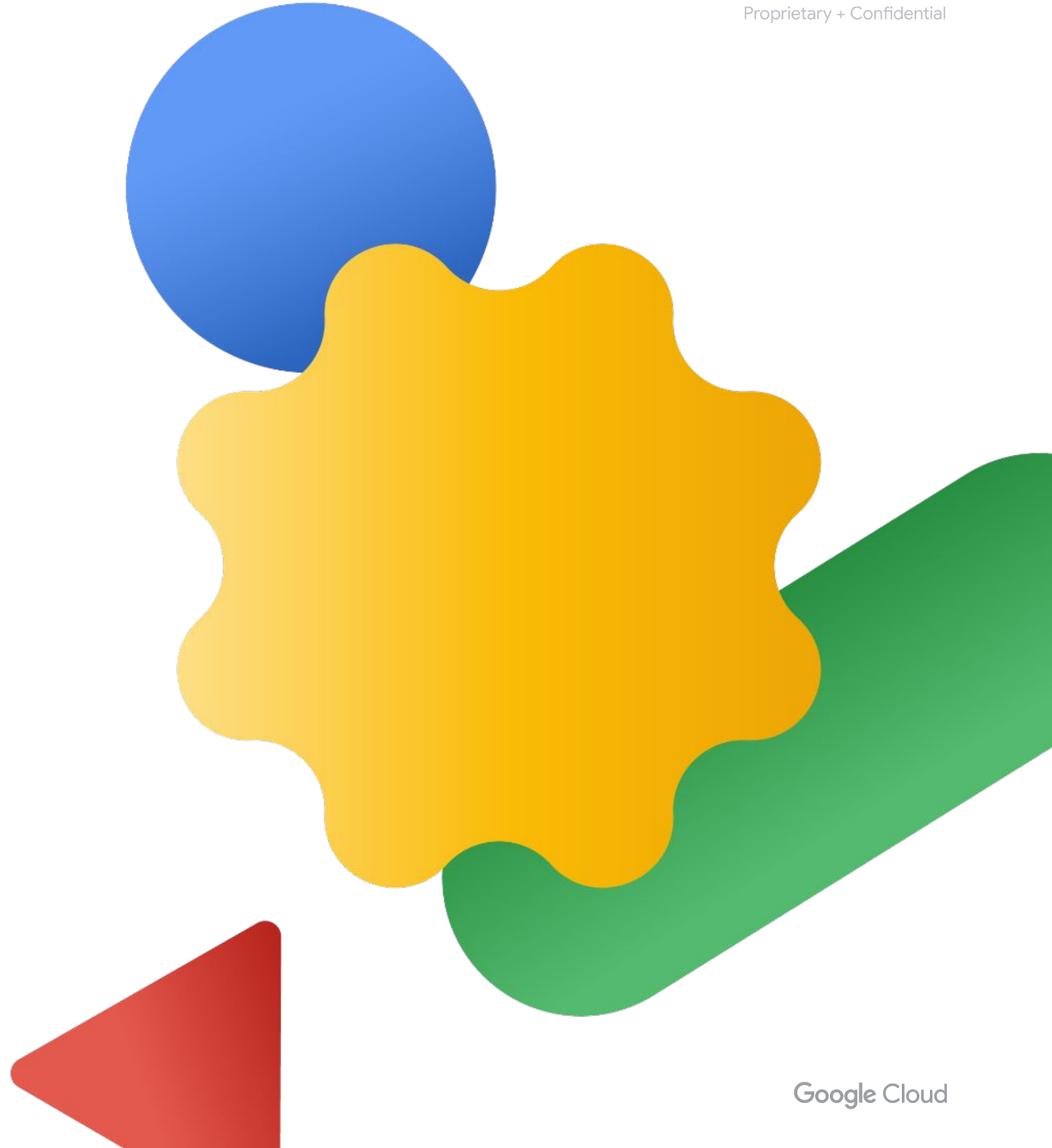


Cloud Secure Web Proxy (SWP)

- Web (HTTP/S) egress traffic inspection, protection, and control
- Managed service (no VMs to set up)
- Explicit proxy (configure clients to use)
- Integrated with Cloud Monitoring/Logging
- Requests can come from:
  - VMs
  - Containers
  - Serverless environments
  - Hybrid workloads connected via VPN/Interconnect

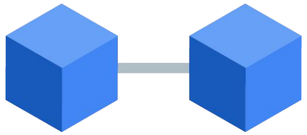
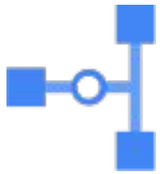
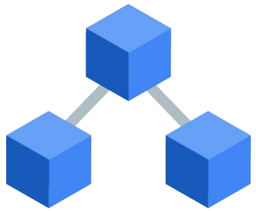
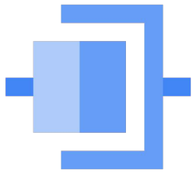


Hybrid connectivity



Google offers various network connectivity options to suit diverse application and workload requirements.

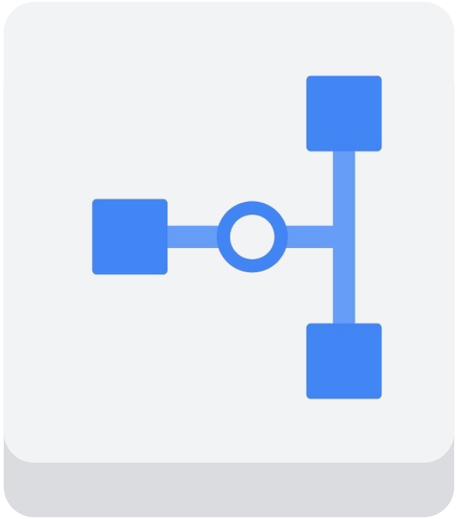
Cloud VPN

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

Cloud VPN

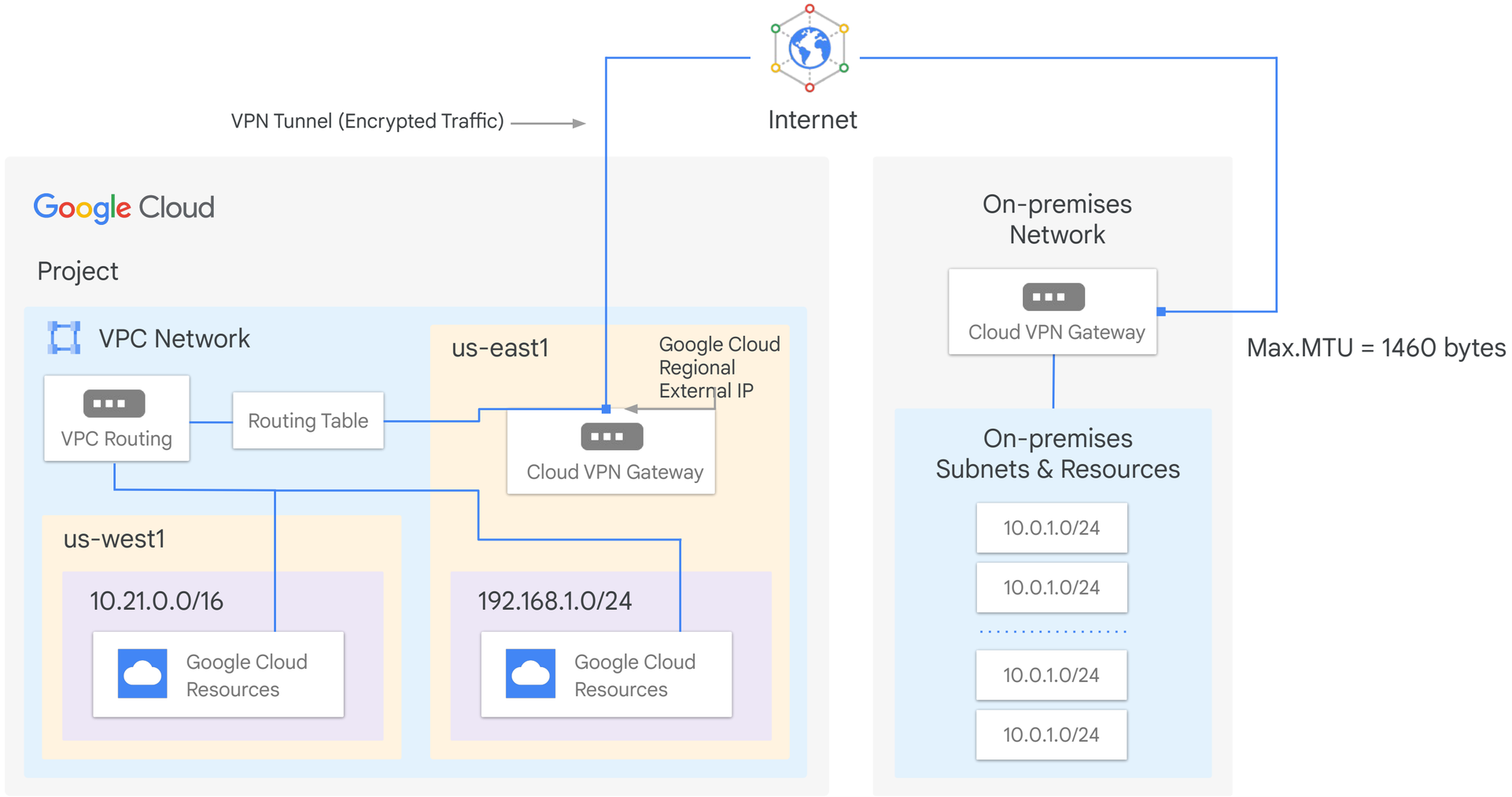
Securely connects your on-premises network to your Google Cloud VPC network

- Useful for low-volume data connections
- Classic VPN: 99.9% SLA
- High-availability (HA) VPN: 99.99% SLA
- Supports:
  - Site-to-site VPN
  - Static routes (Classic VPN only)
  - Dynamic routes (Cloud Router)
  - IKEv1 and IKEv2 ciphers



Cloud VPN

Classic VPN topology



HA VPN overview

Availability

- Provides 99.99% service availability.

IP addresses

Google Cloud automatically chooses two external IP addresses:

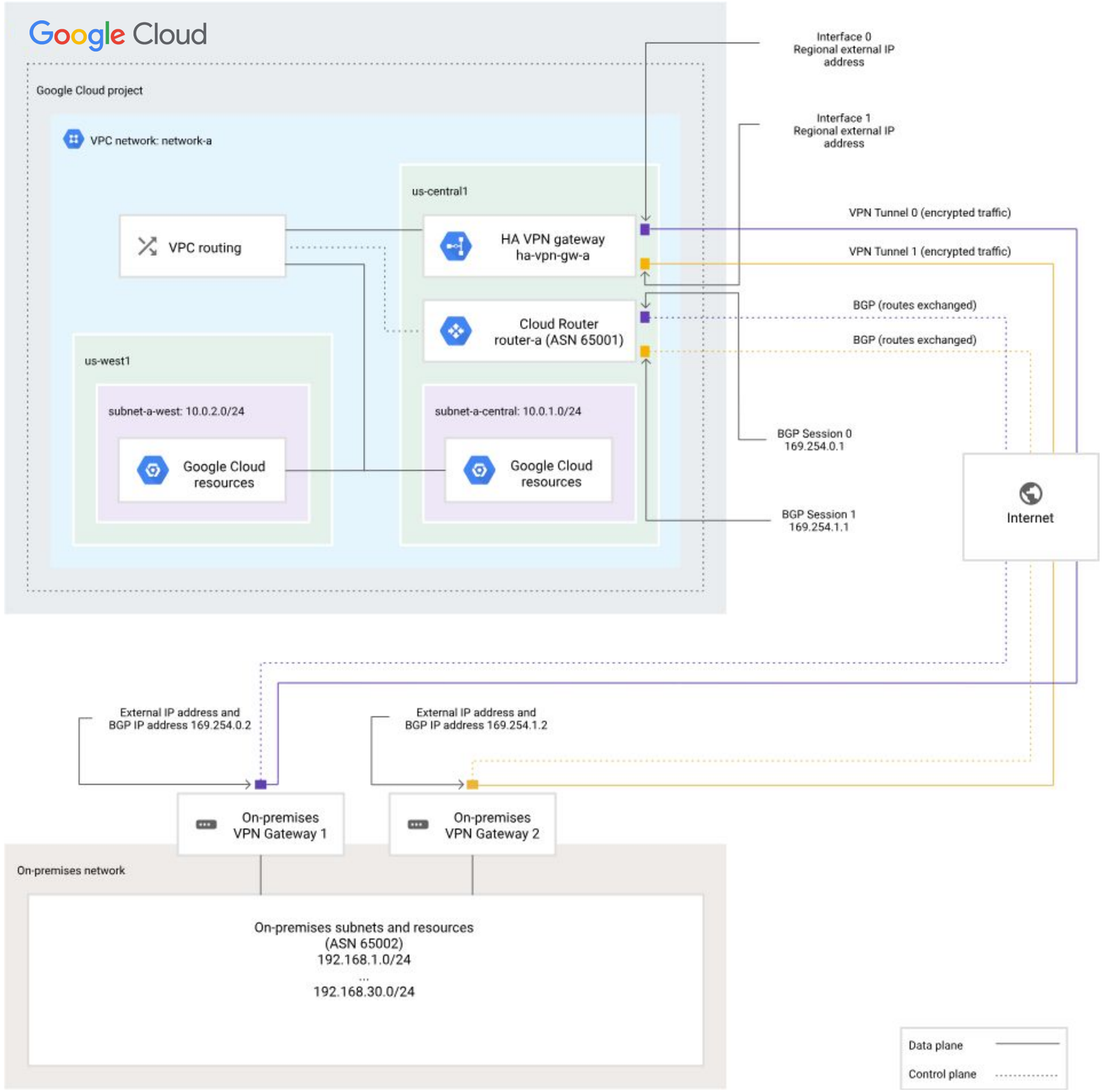
- Supports multiple tunnels
- VPN tunnels connected to HA VPN gateways must use dynamic (BGP) routing

Site-to-site VPN

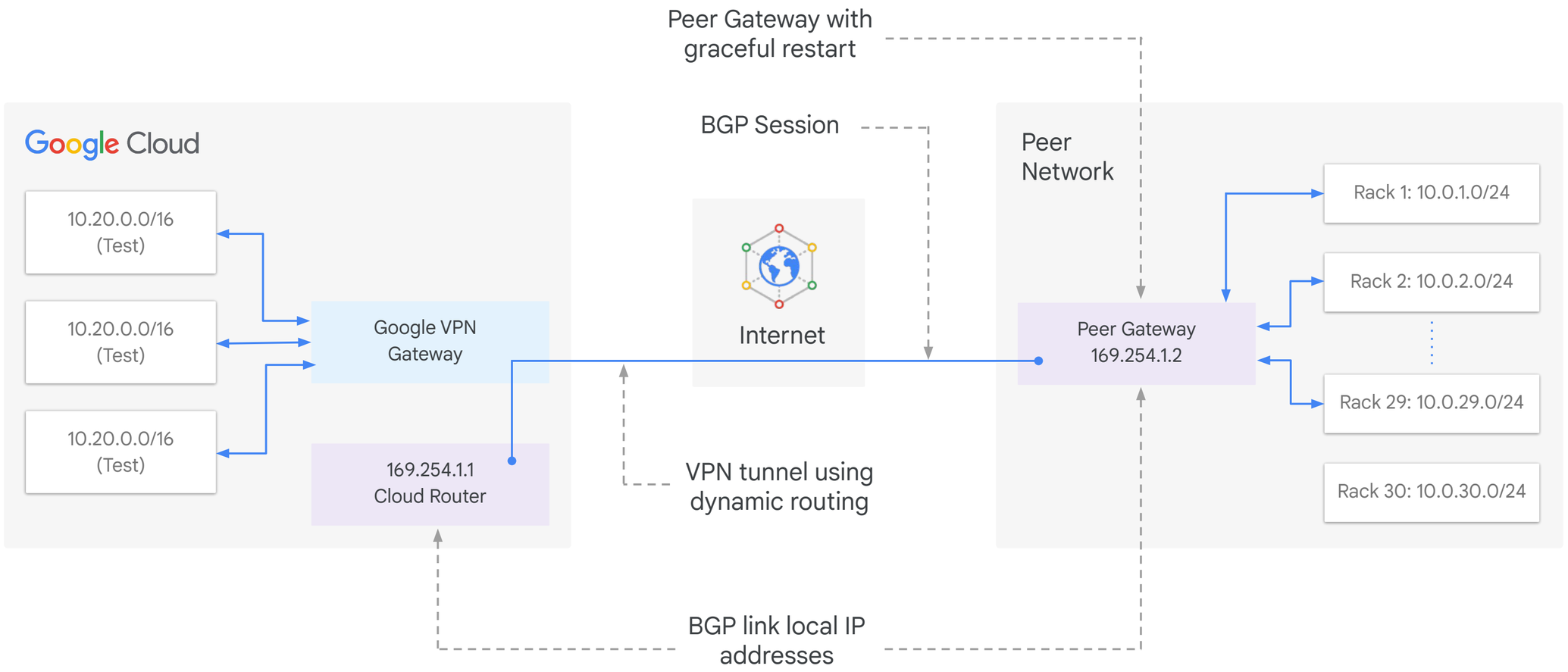
Supports site-to-site VPN for different topologies/configuration scenarios:

- An HA VPN gateway to peer VPN devices
- An HA VPN gateway to an Amazon Web Services (AWS) virtual private gateway
- Two HA VPN gateways connected to each other

HA VPN to peer VPN gateway topology

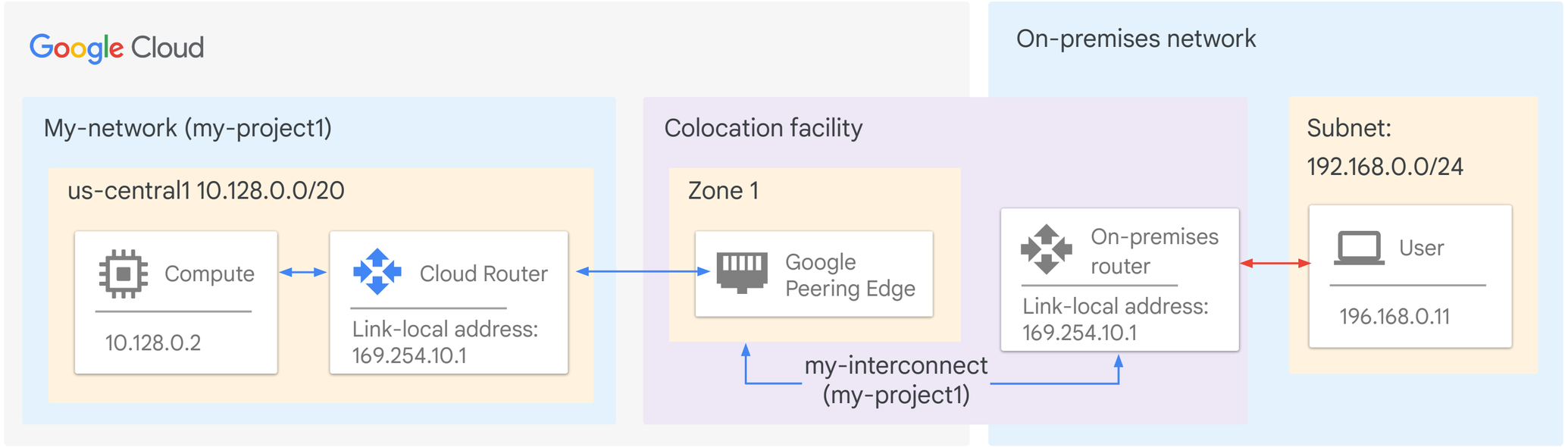


Dynamic routing with Cloud Router



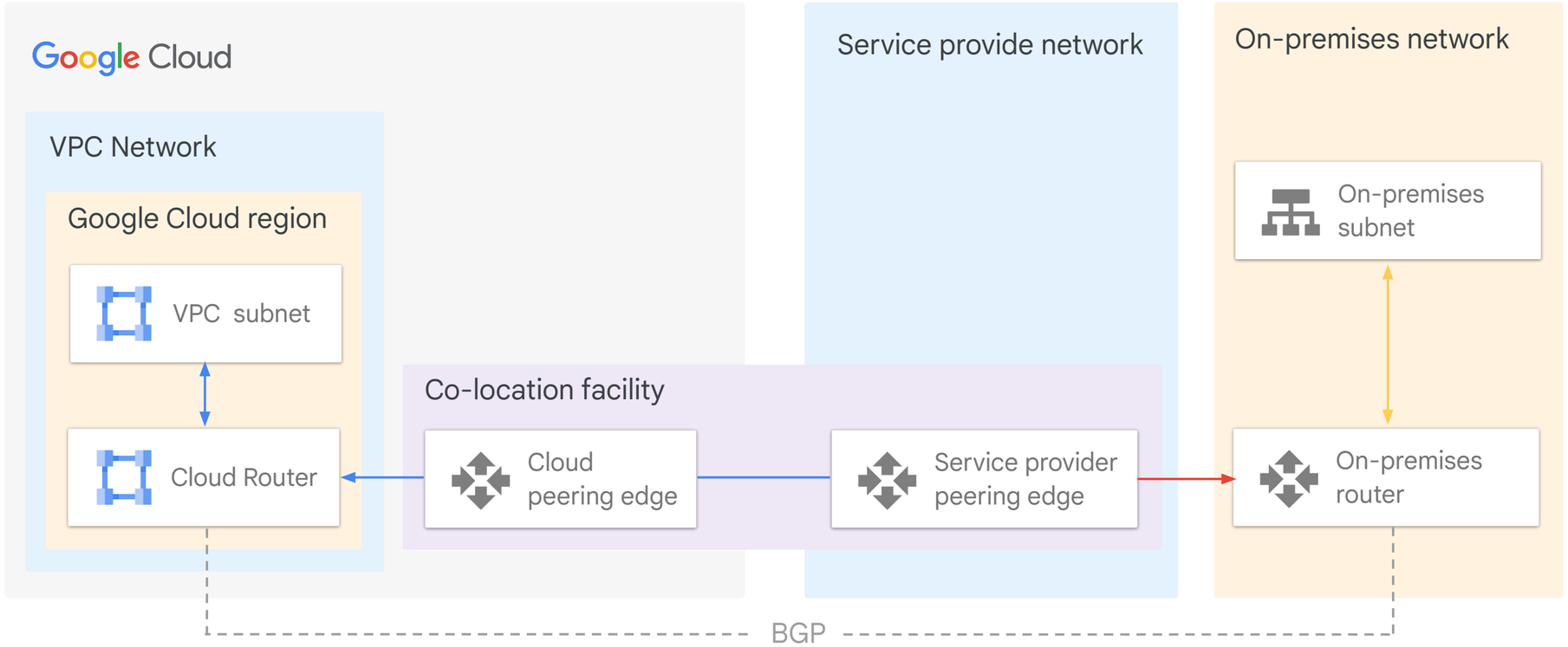
Dedicated Interconnect

Provides direct physical connections

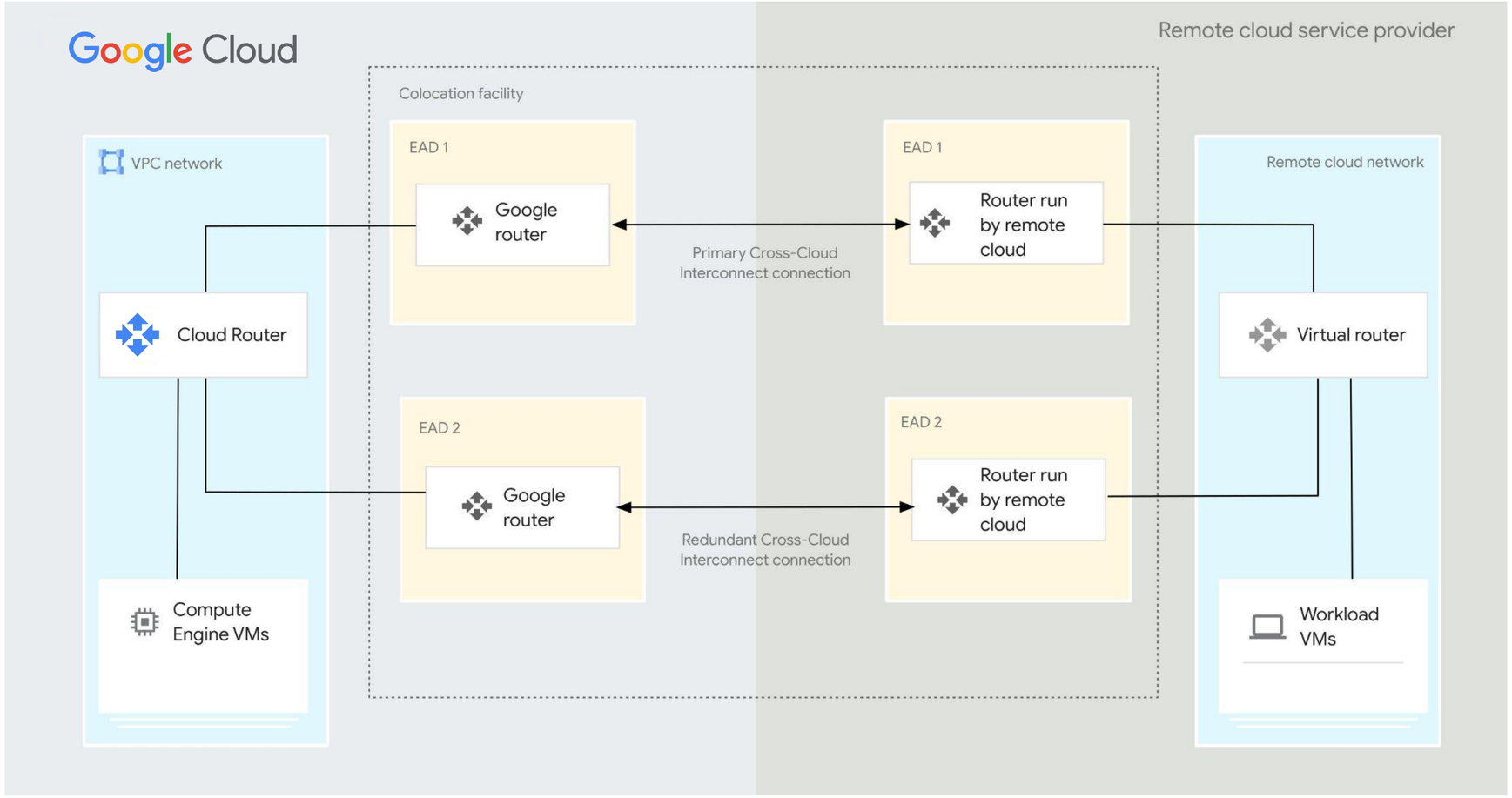


Partner Interconnect

Provides connectivity through a supported service provider



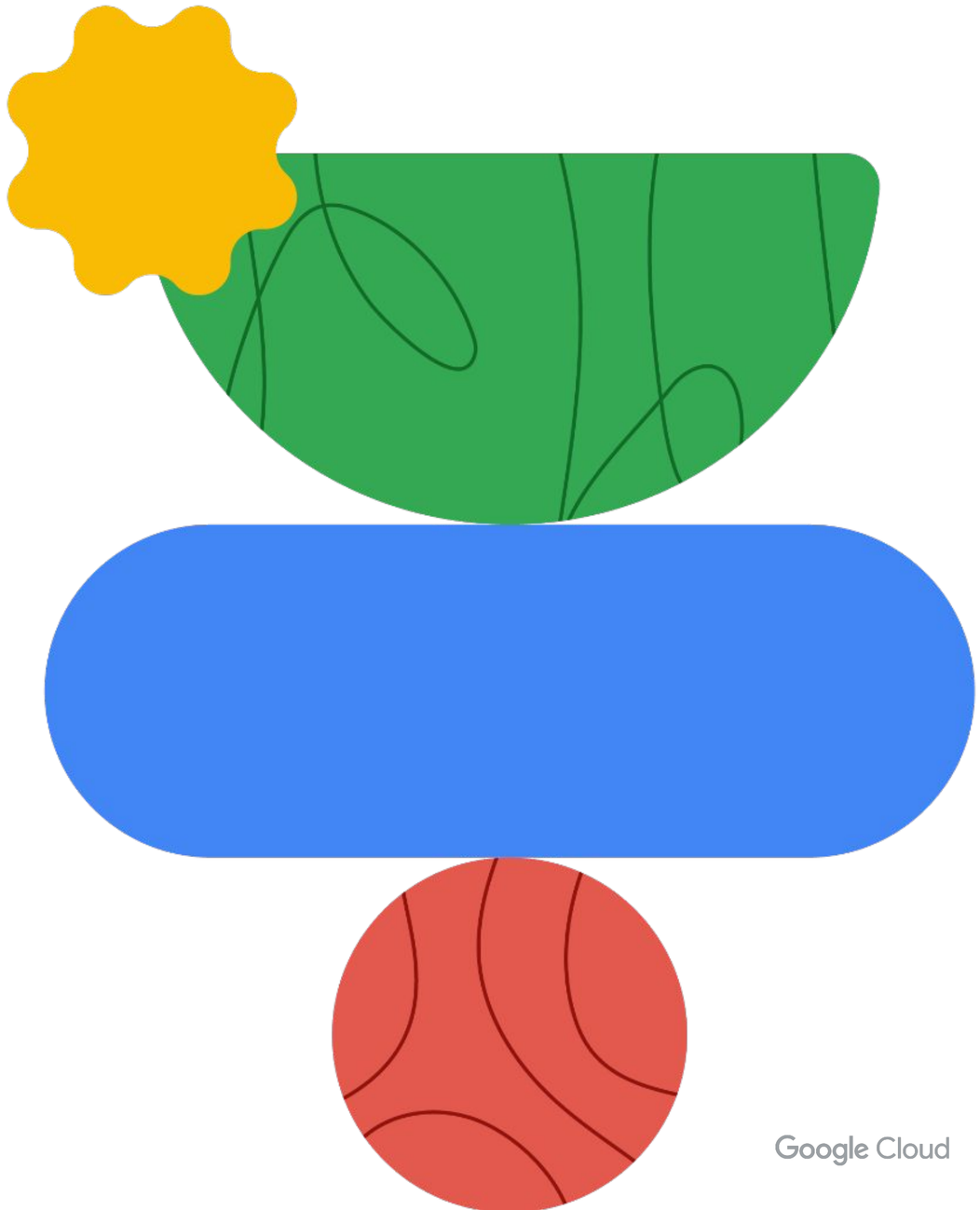
Cross Cloud Interconnect



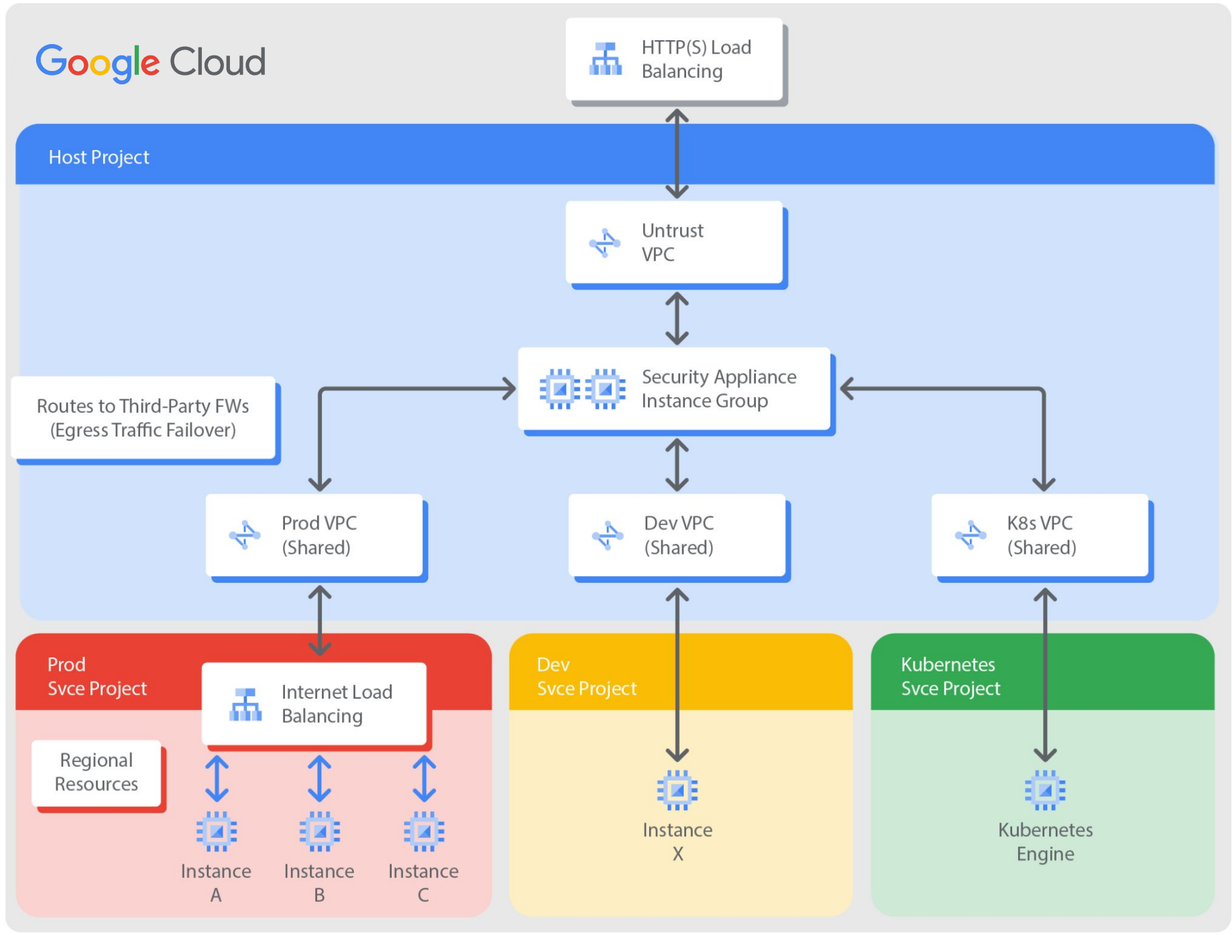
Comparison of Interconnect options

Connection	Provides	Capacity	Requirements	Access Type
IPsec VPN tunnel	Encrypted tunnel to VPC networks through the public internet	1.5-3 Gbps per tunnel	On-premises VPN gateway	Internal IP addresses
Dedicated Interconnect	Dedicated, direct connection to VPC networks	10 Gbps or 100 Gbps per link	Connection in colocation facility	
Partner Interconnect	Dedicated bandwidth, connection to VPC network through a service provider	50 Mbps – 10 Gbps per connection	Service provider	

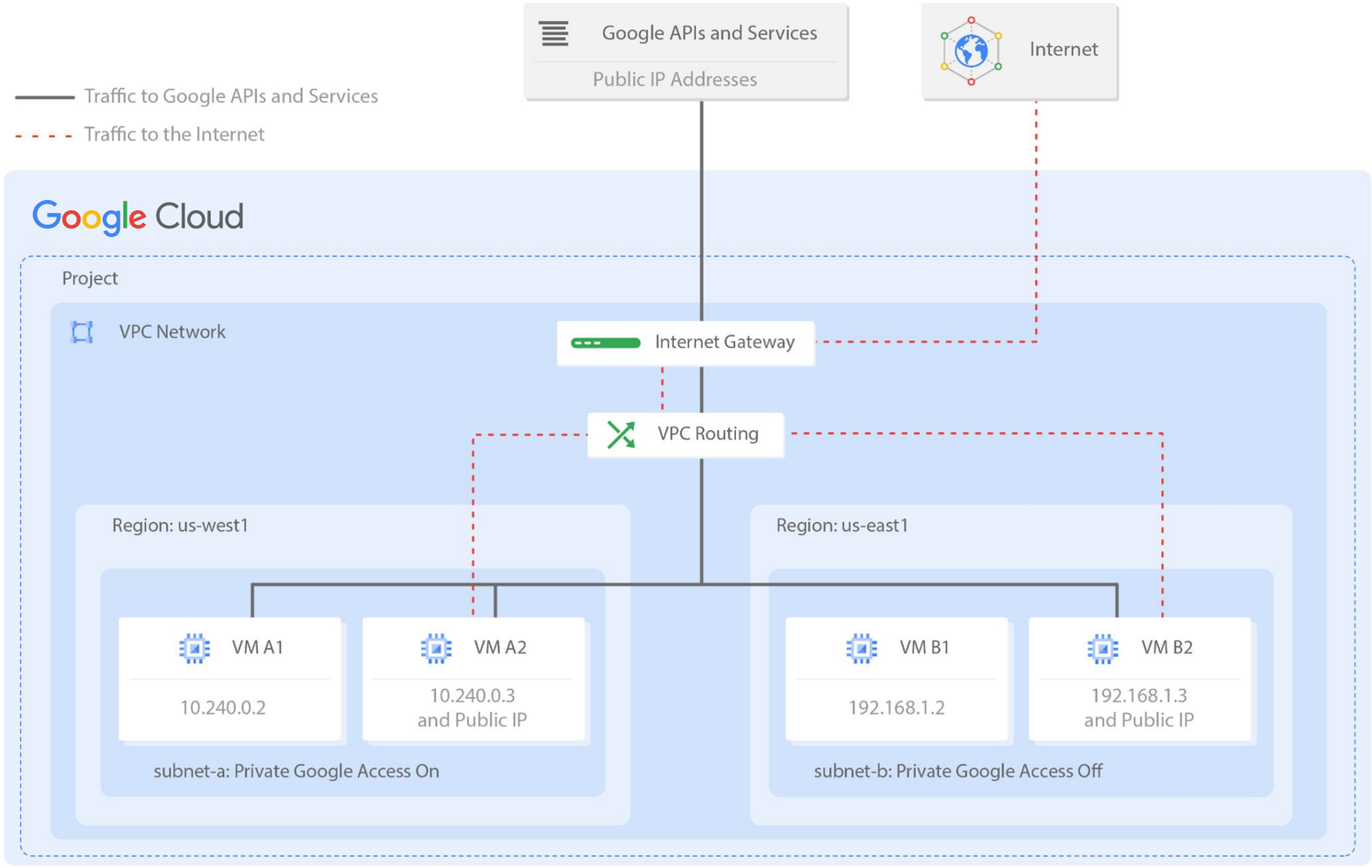
Networking design and deployment



Use security appliance for next-generation firewall



Private Google Access to Google APIs and services

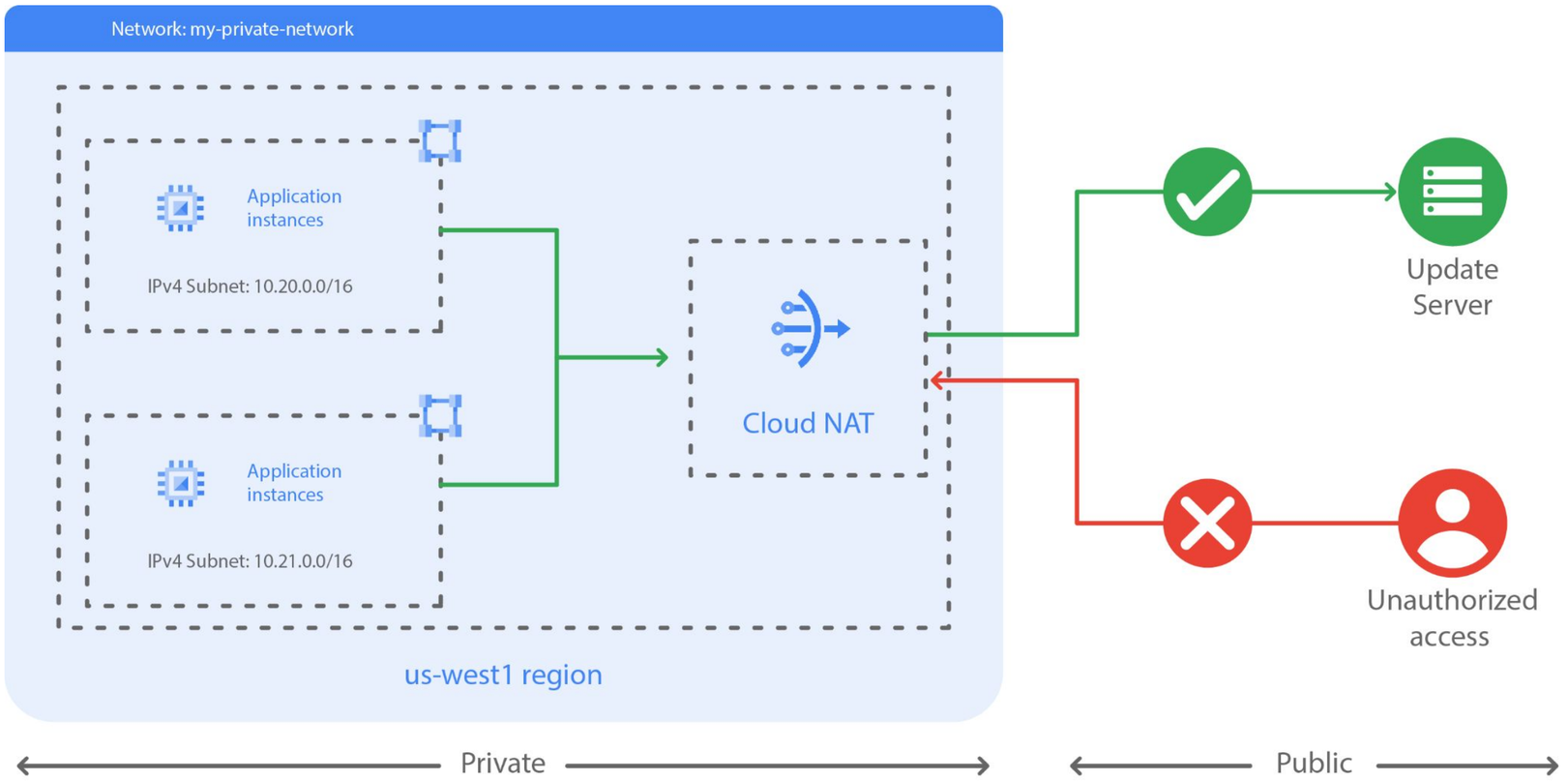


Different private access options

Option	Connection	Usage
Private Google Access	Connect to the public IP addresses of Google APIs and services through the VPC network's default internet gateway.	Connect to Google APIs and services without giving your Google Cloud resources external IP addresses.
Private Google Access for on-premises hosts	Connect to the public IP addresses of Google APIs and services through a VPN tunnel, or interconnect by using a restricted IP address range.	Connect to Google APIs and services through a VPC network without requiring your on-premises hosts to have external IP addresses.
Private services access	Connect to a Google or a third-party managed VPC network through a VPC Peering connection.	Connect to specific Google and third-party services without assigning external IP addresses to your Google Cloud and Google or third-party resources.

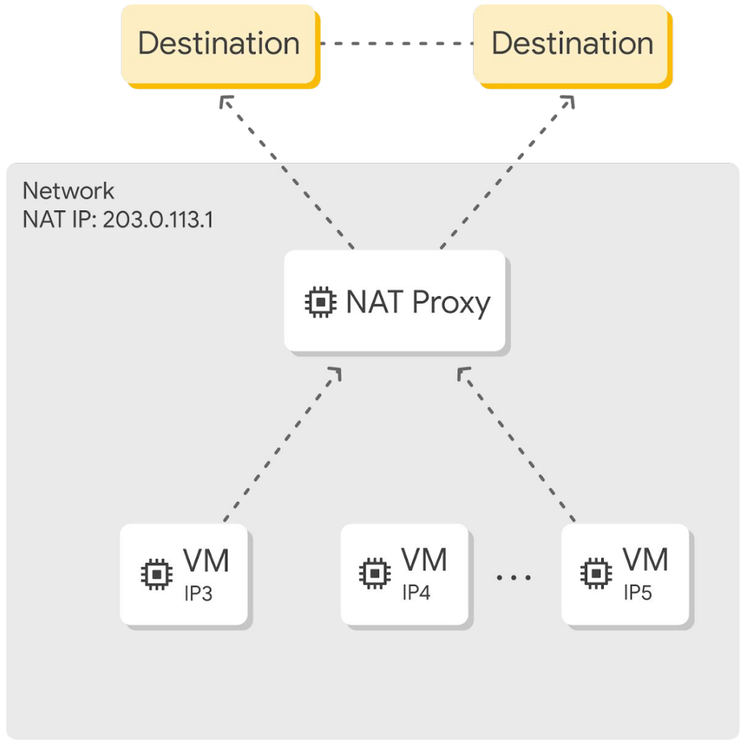
Cloud NAT

Provides internet access to private instances

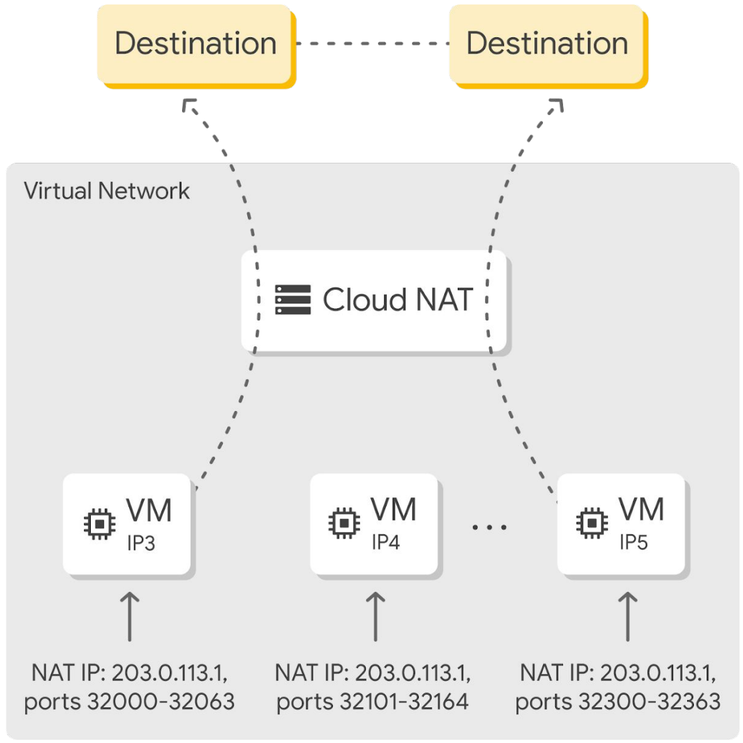


Cloud NAT

Is a fully managed, software-defined service

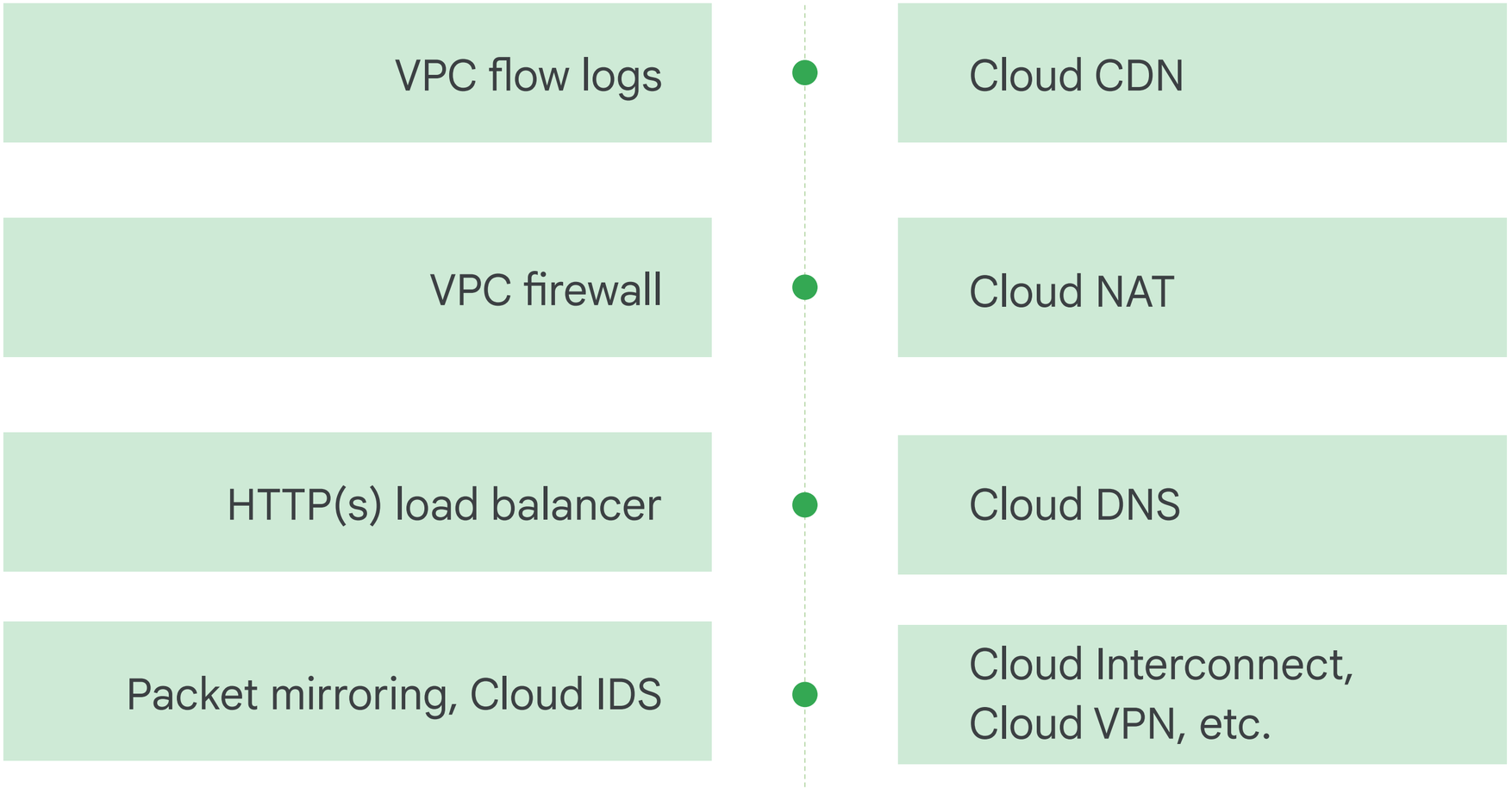


1. Typical NAT Proxies



2. Google Cloud NAT

Network logging



Packet Mirroring

Packet mirroring identifies anomalous network traffic, including malware, data exfiltration, and lateral movement.

Clones traffic

Packet mirroring clones the traffic of specific instances in your VPC network and forwards it for examination (Compute Engine Collectors)

Captures traffic

Captures all ingress/egress traffic and packet data, such as payloads and headers.

Exports traffic

Exports all traffic, not only the traffic between sampling periods.

Packet Mirroring

Use security software to analyze mirrored traffic to detect threats or anomalies

IDS tools

IDS tools can analyze multiple packets to match a signature to detect persistent threats.

Security software

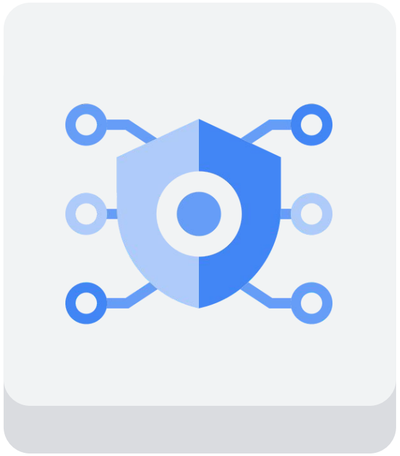
Inspects packet payloads to detect protocol anomalies.

Network forensics

Network forensics for PCI compliance and other regulatory use cases.

Google Cloud IDS Service

- **Cloud-native managed NG-IDS** for advanced network security and compliance needs
- **Ease of setup and management**, high performance, and availability
- **Advanced Threat Detection powered by Palo Alto Networks** – detect exploit attempts, evasion techniques, port scans, buffer overflows, protocol fragmentation, and obfuscation attempts
- **Alerts in UI and Cloud Logging**, integrations with SIEM/SOAR partners



Google Cloud IDS Service

Google Cloud

Simple, cloud-scale native service with best-in-class infrastructure

+

paloalto NETWORKS

Best-in-class security for advanced threats

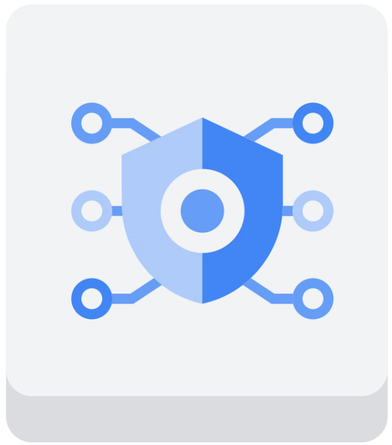
=

Simple, cloud-scale, native, best-in-class security for customers

Cloud IDS - Overview

Cloud IDS

Provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network



- Cloud-native, easy and fast to deploy, and managed network threat detection
- Creates a Google-managed peered network with mirrored VMs and inspected to provide advanced threat detection
- Provides full visibility into network traffic, letting you monitor VM-to-VM communication
- Meets your advanced threat detection and compliance requirements, including PCI 11.4.

Cloud IDS

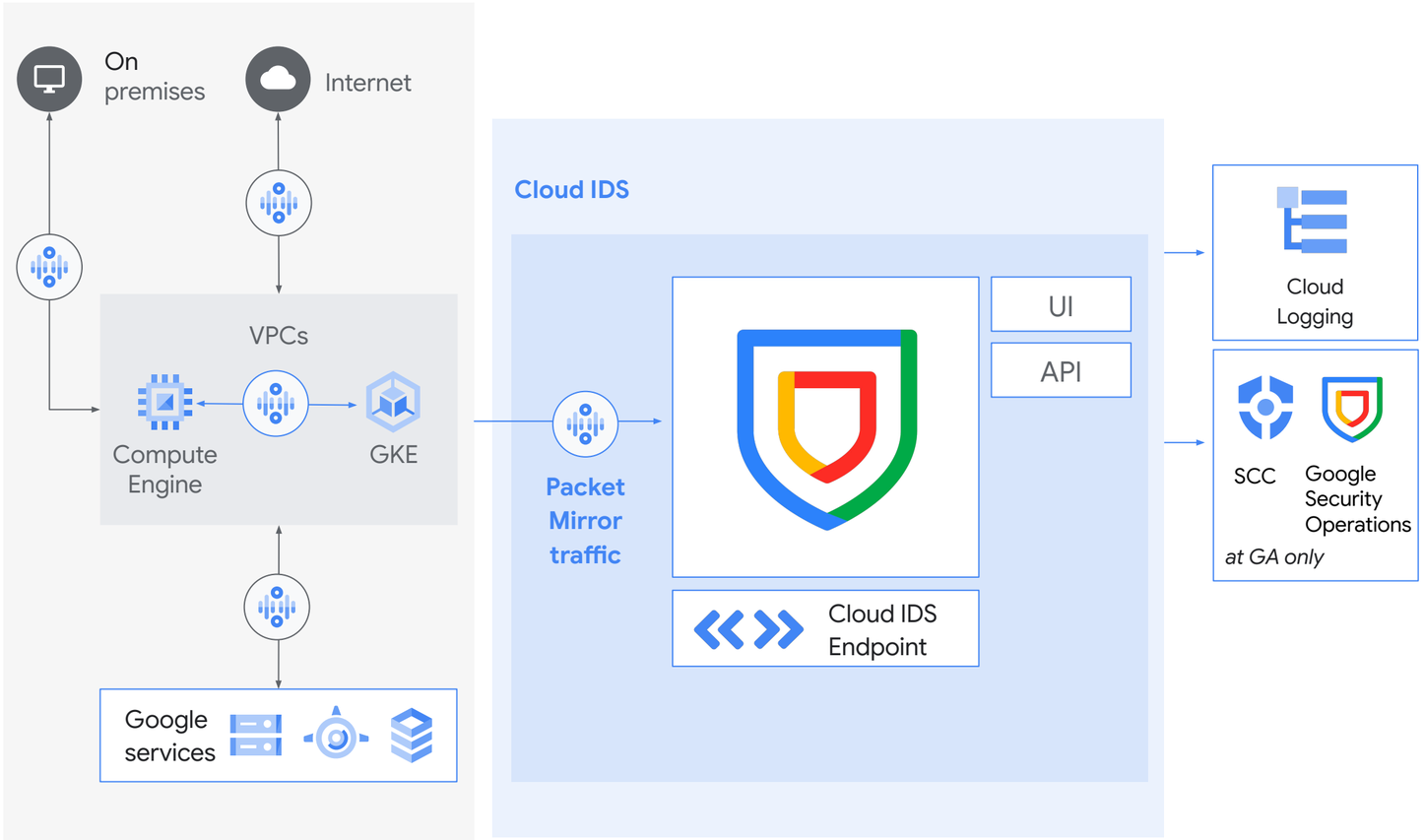
Endpoints and packet mirroring

IDS endpoint

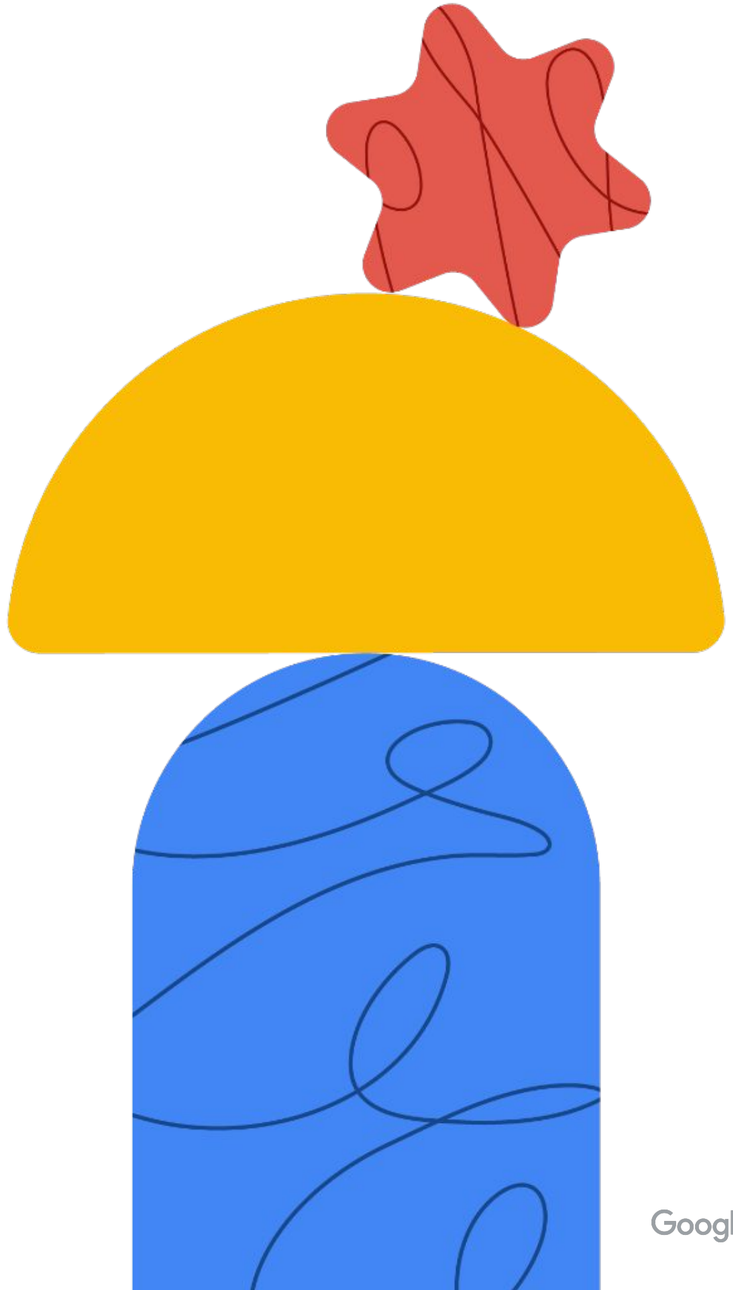
- Zonal resource that inspects traffic from any zone in its region
- Receives mirrored traffic and performs threat detection analysis

Packet mirroring

- Creates a copy of your network traffic
- Attack packet mirroring policies to IDS endpoints



VPC-Service Controls (VPC-SC) security perimeters



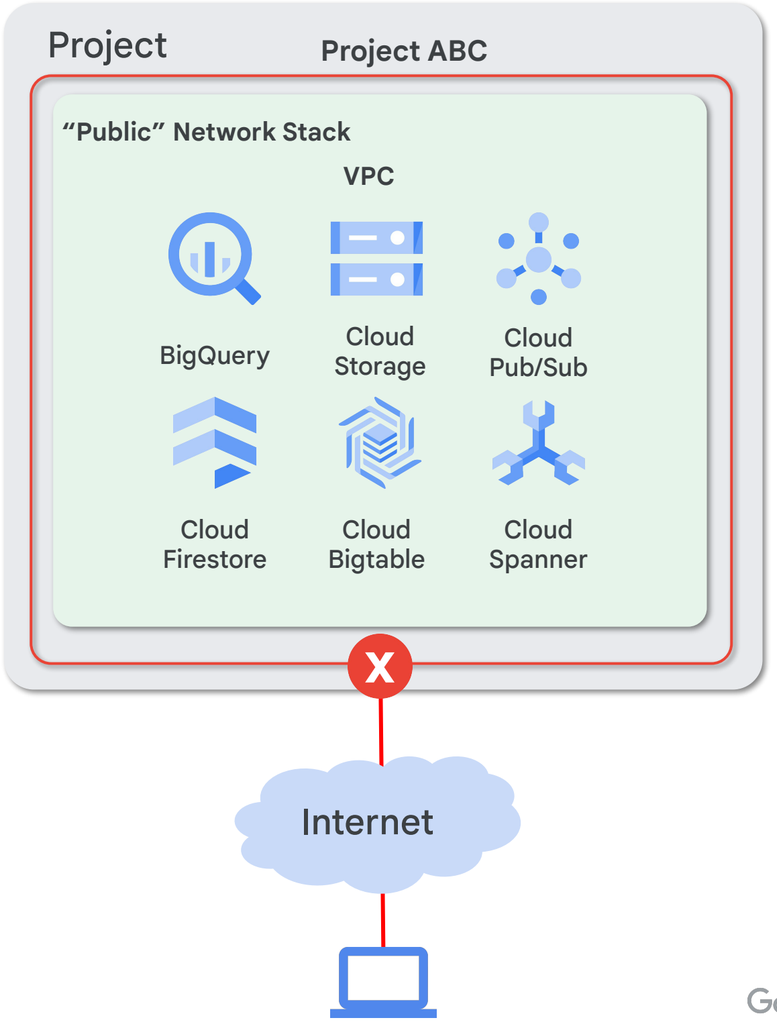
VPC Service Controls

Helps prevent data exfiltration and controlling access to Google APIs

Isolate resources of multi-tenant Google Cloud services to **mitigate data exfiltration risks**.

Enforce **adaptive access control based on IP range or device trust (BeyondCorp)** for Google Cloud resource access from outside privileged networks.

Configure private, efficient, and **secure data exchange** across organizations and OUs.



VPC Service Control

The main building blocks

Perimeter

Access level

Private Google Access

Perimeter bridge

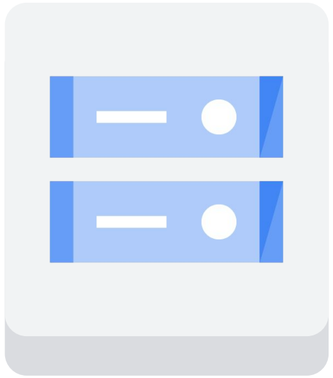
Ingress/egress policies

VPC Service Control

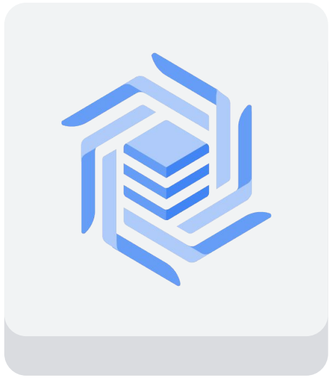
The main building blocks

Supported Google APIs that are used the most

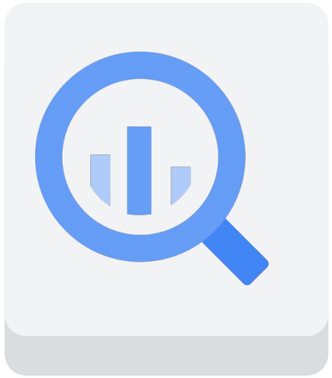
Unsupported services



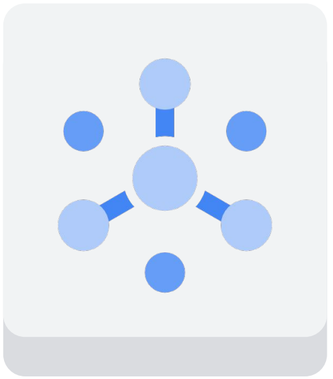
Cloud Storage



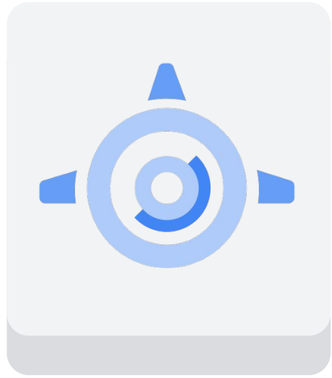
Cloud Bigtable



BigQuery



Pubsub



App Engine

VPC Service Control

Perimeter and access level

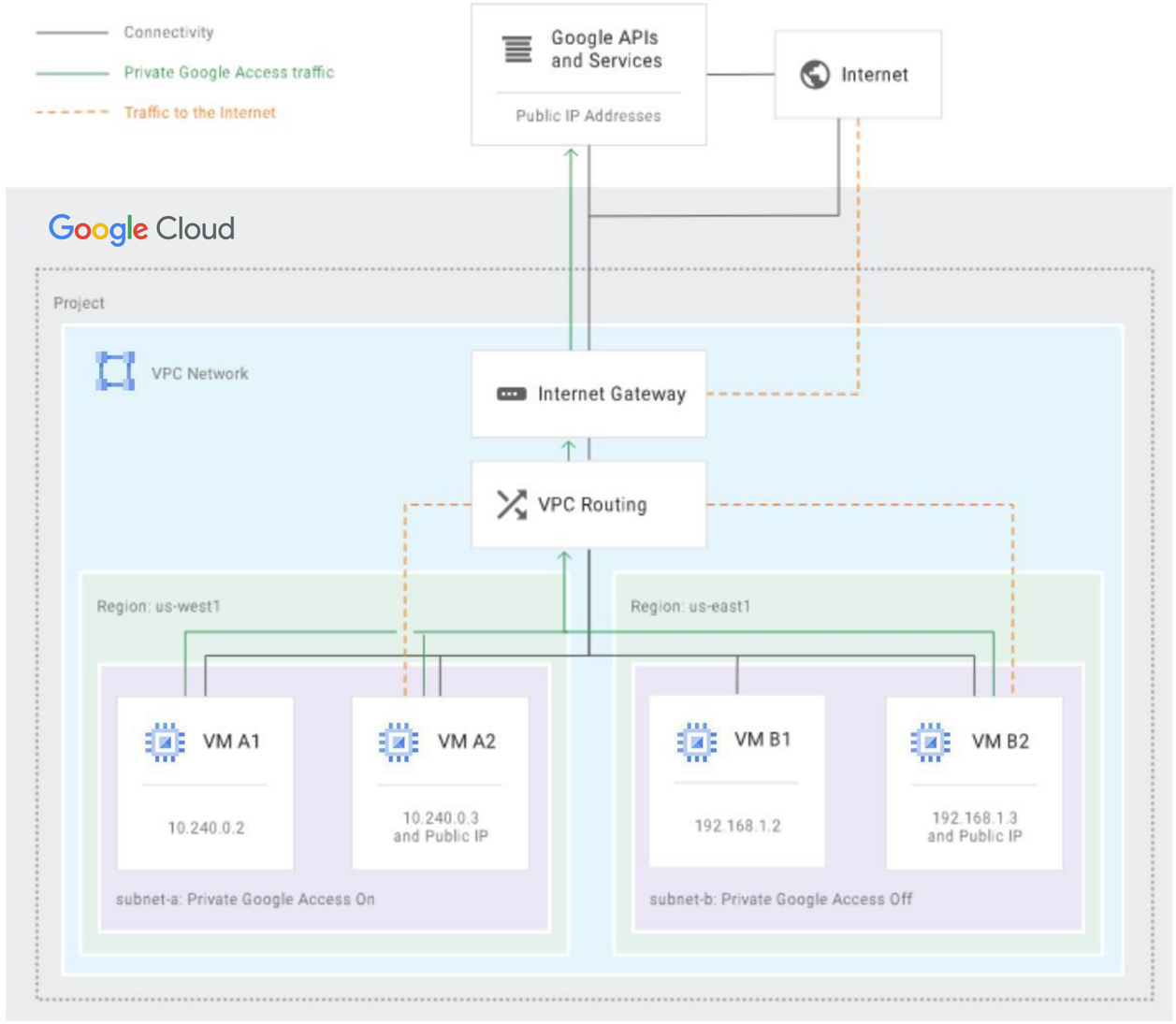
Perimeter

- Projects are added to a perimeter individually and each project can only be in one perimeter.
- Perimeter is managed at the organizational level (max 50 perimeters).
- Services need to be explicitly enabled to be “protected”.

Access level

- Through Access Context Manager, access levels are created to define access rules, with fine-grained access control based on a variety of attributes:
  - IP subnetworks
  - Regions
  - Members (users/SA)
  - Device policy
- Max 30 rules

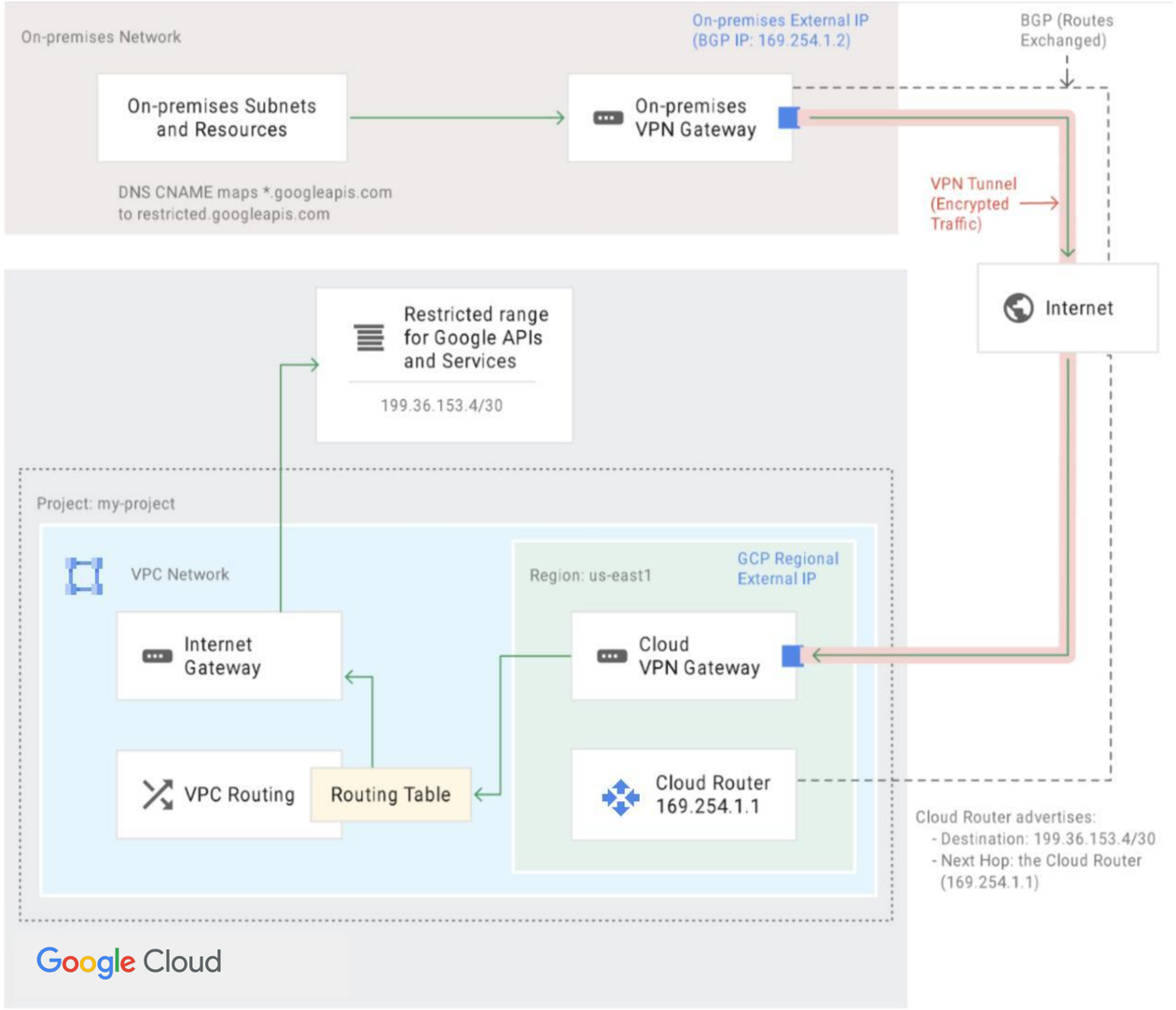
Private Google Access from Google Cloud



Private Google acces:

Private Compute Engine instances accessing Google APIs Disabled by default

Private Google Access from on-premises



Private Google access from on-premises:

On-premises using the private link (Cloud VPN or Cloud Interconnect) between the customer data centers and Google Cloud to reach Google APIs.

Two VIPS can be used:

- **restricted.googleapis.com**: only APIs that support VPC Service Controls
- **private.googleapis.com**: all Google APIs

VPC Service Control

Perimeter bridge and ingress/egress policies

Perimeter bridge

- A project can be assigned to only one perimeter.
- A project in a perimeter can be added to a perimeter bridge to be able to communicate with projects in another perimeter.
- A project can be added to multiple perimeter bridges.
- A perimeter bridge can have multiple projects (max 10k projects).

Ingress/egress policies

- The ingress and egress rule blocks specify the direction of allowed access to and from different identities and resources.
- Ingress and egress rules can replace and simplify use cases that previously required one or more perimeter bridges.

Access Context Manager

Access levels

Attributes
Context of the user and request

- Employee
- Device
- Location

Policy
Define and apply policies

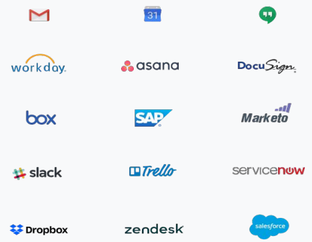
Rules engine

Apps and Data
Protect all critical data

Google Cloud

APIs, Resources, Apps

Google Workspace



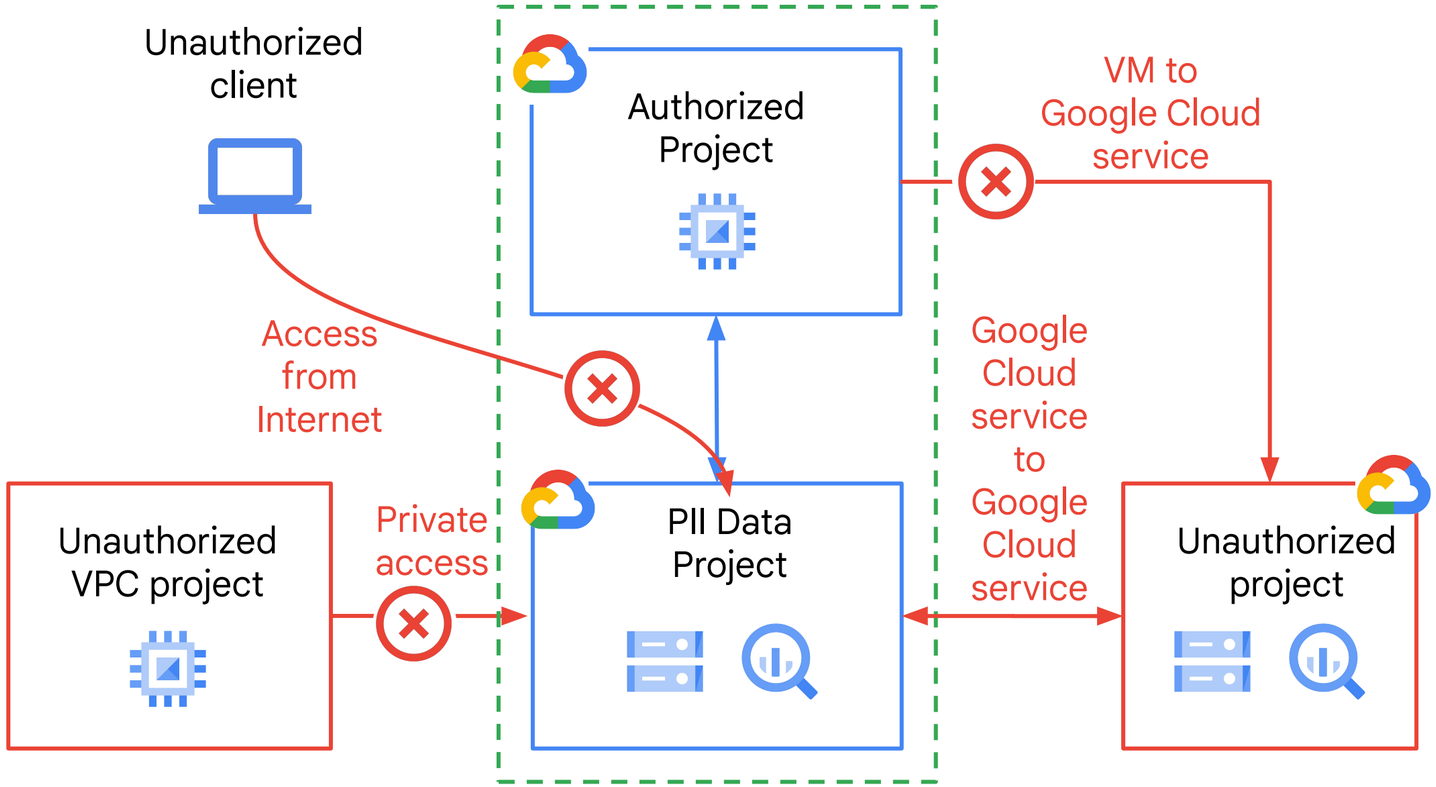
User + Device + Context is the new security perimeter

VPC Service Controls

Service perimeter

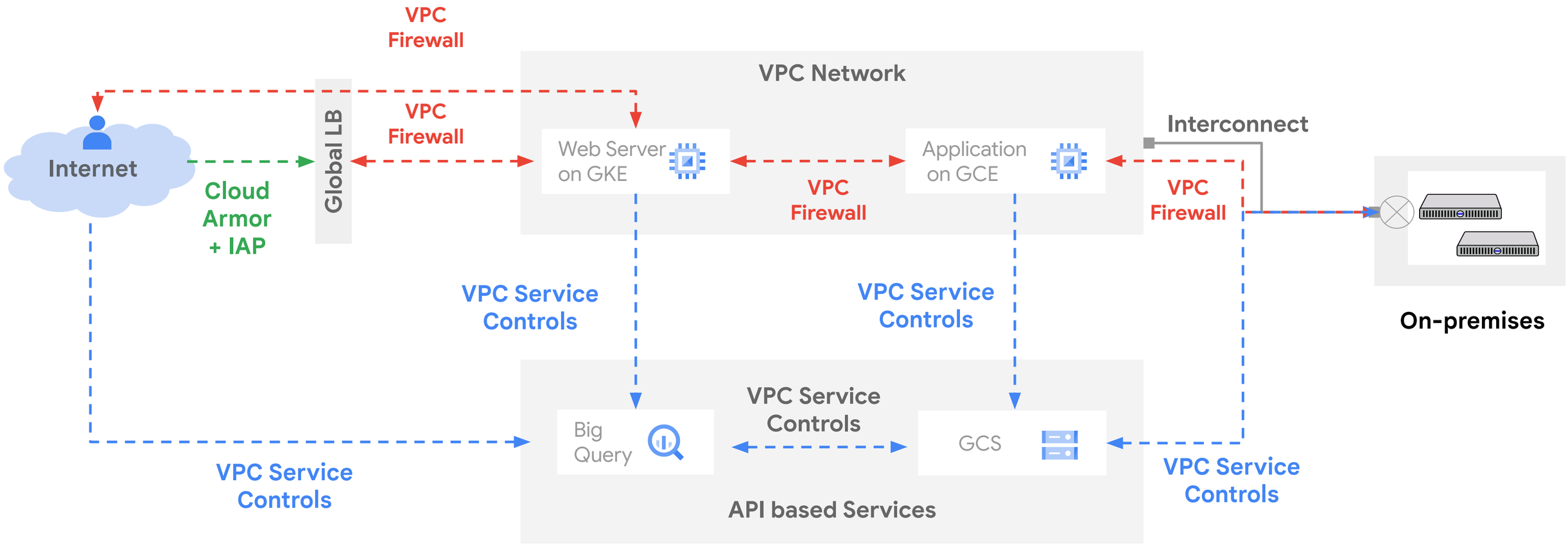
Extend perimeter security to managed Google Cloud services

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



VPC Service Controls

Example architecture



VPC Service Controls versus VPC Firewall

	VPC Firewall	VPC Service Control
Control path	VM ⟷ VM VM ⟷ Internet VM ⟷ On-premises	Google Cloud Service ⟷ VM Google Cloud Service ⟷ Internet Google Cloud Service ⟷ On-premises Google Cloud Service ⟷ Google Cloud Service
Conditions	5-tuple VM tags VM service accounts	VPC network Google Cloud 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


Google Cloud