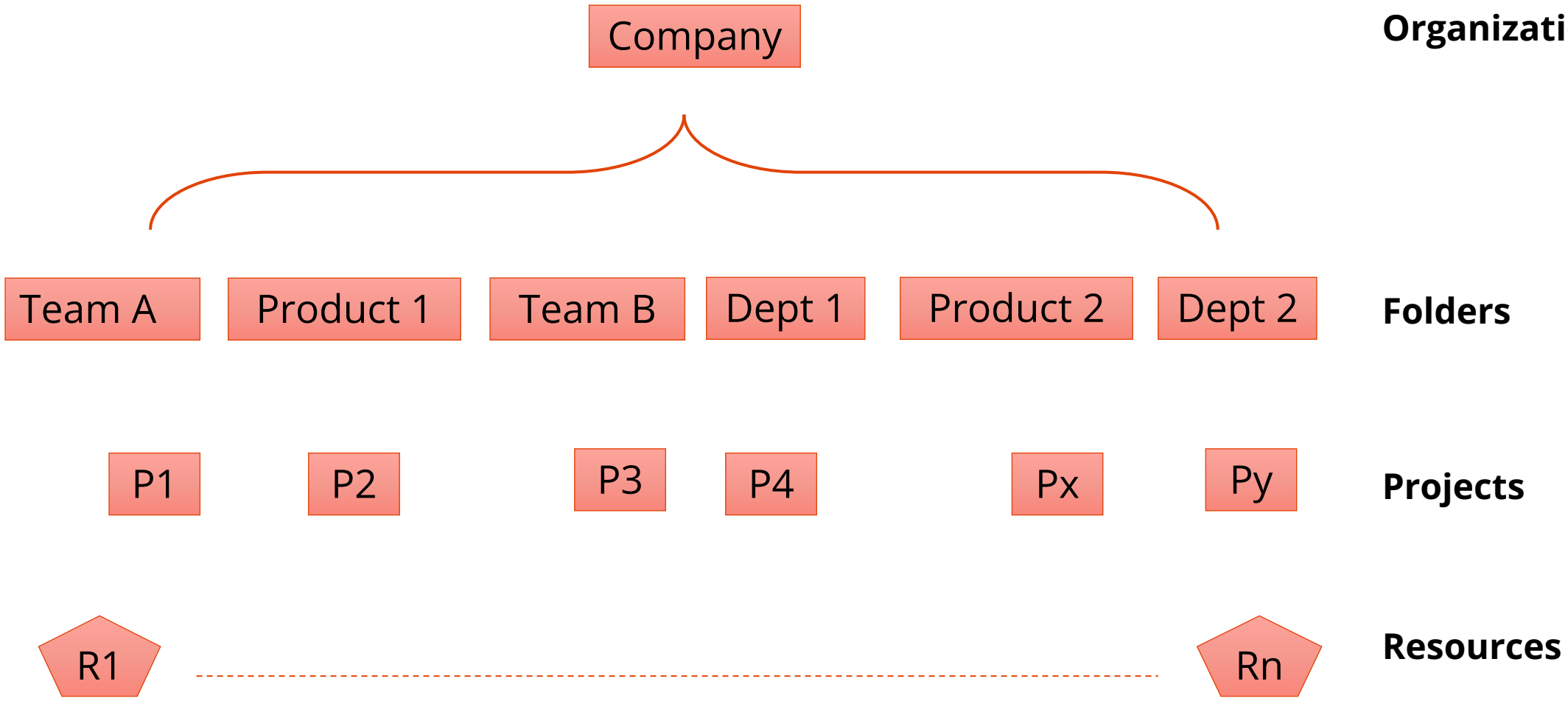
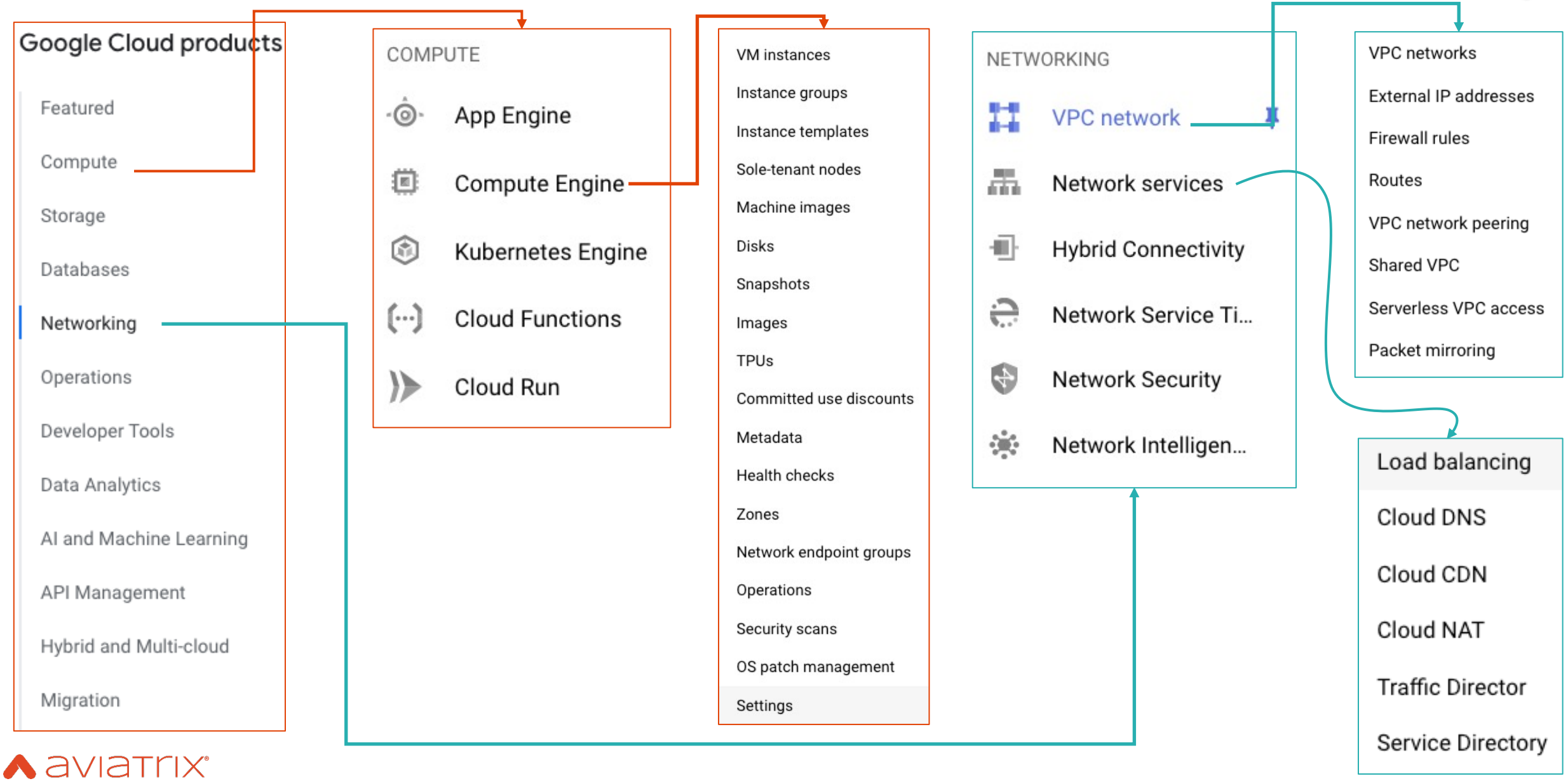
GCP Networking 101

ACE Solutions Architecture Team

GCP Hierarchy



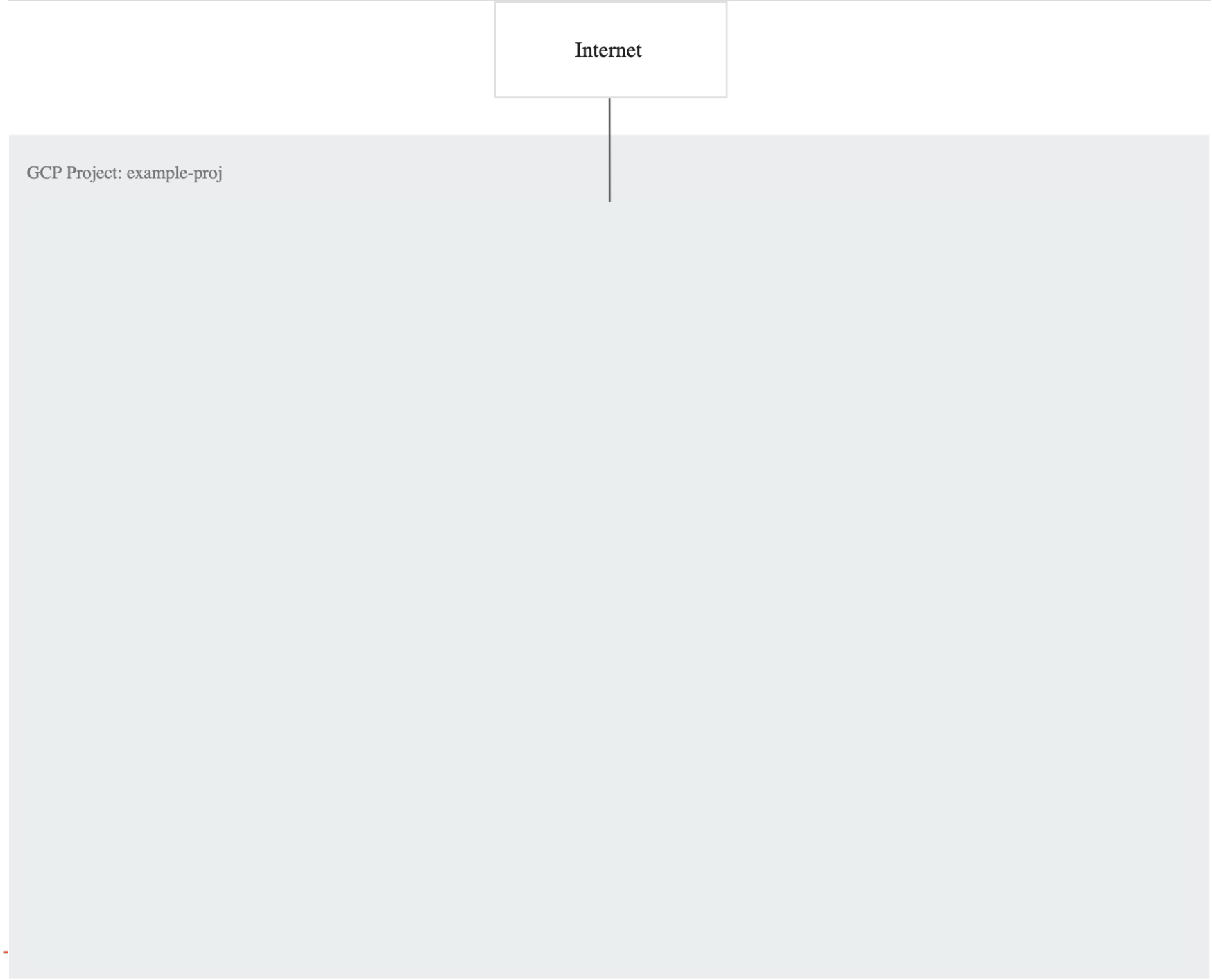
GCP Products and Services

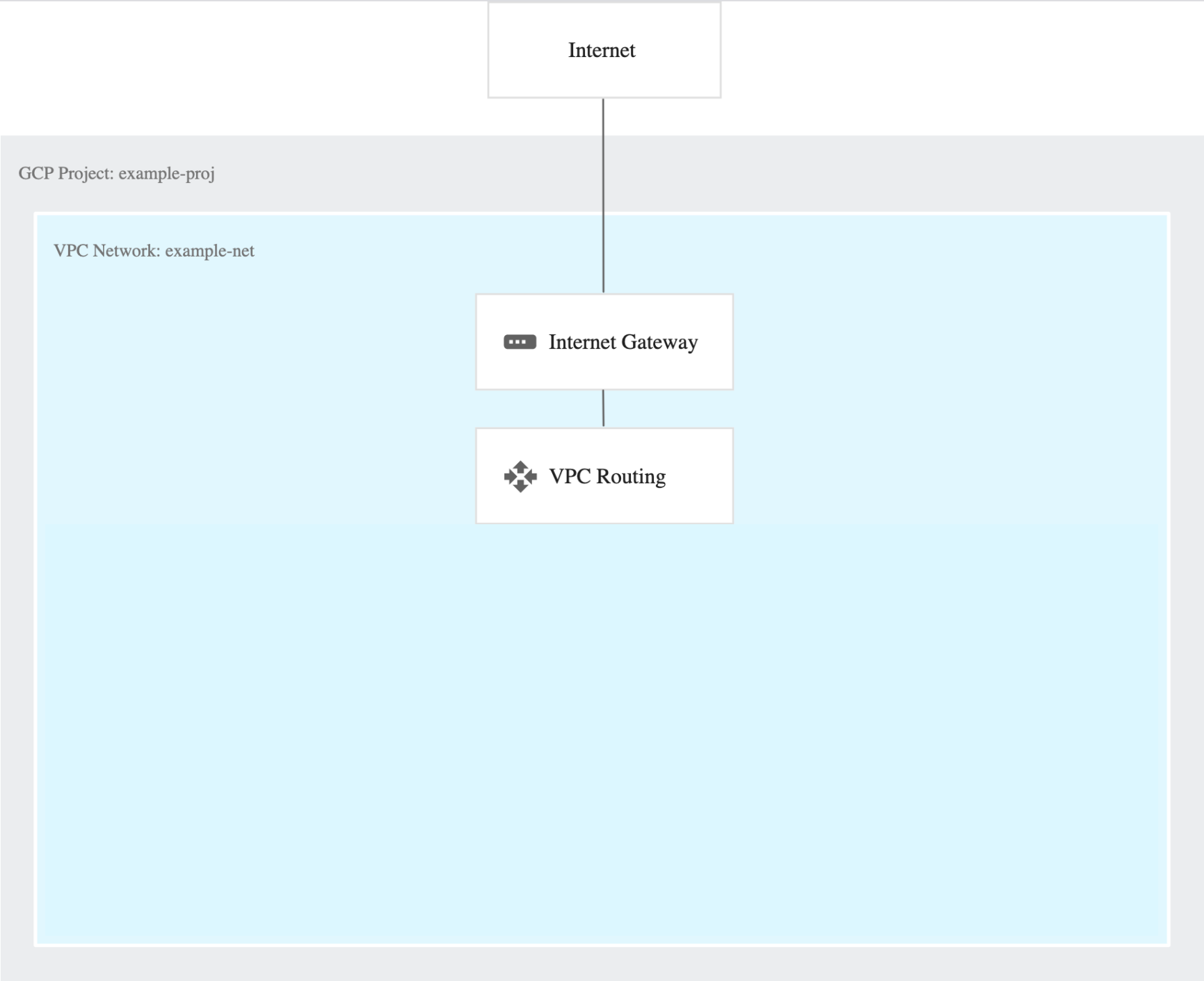


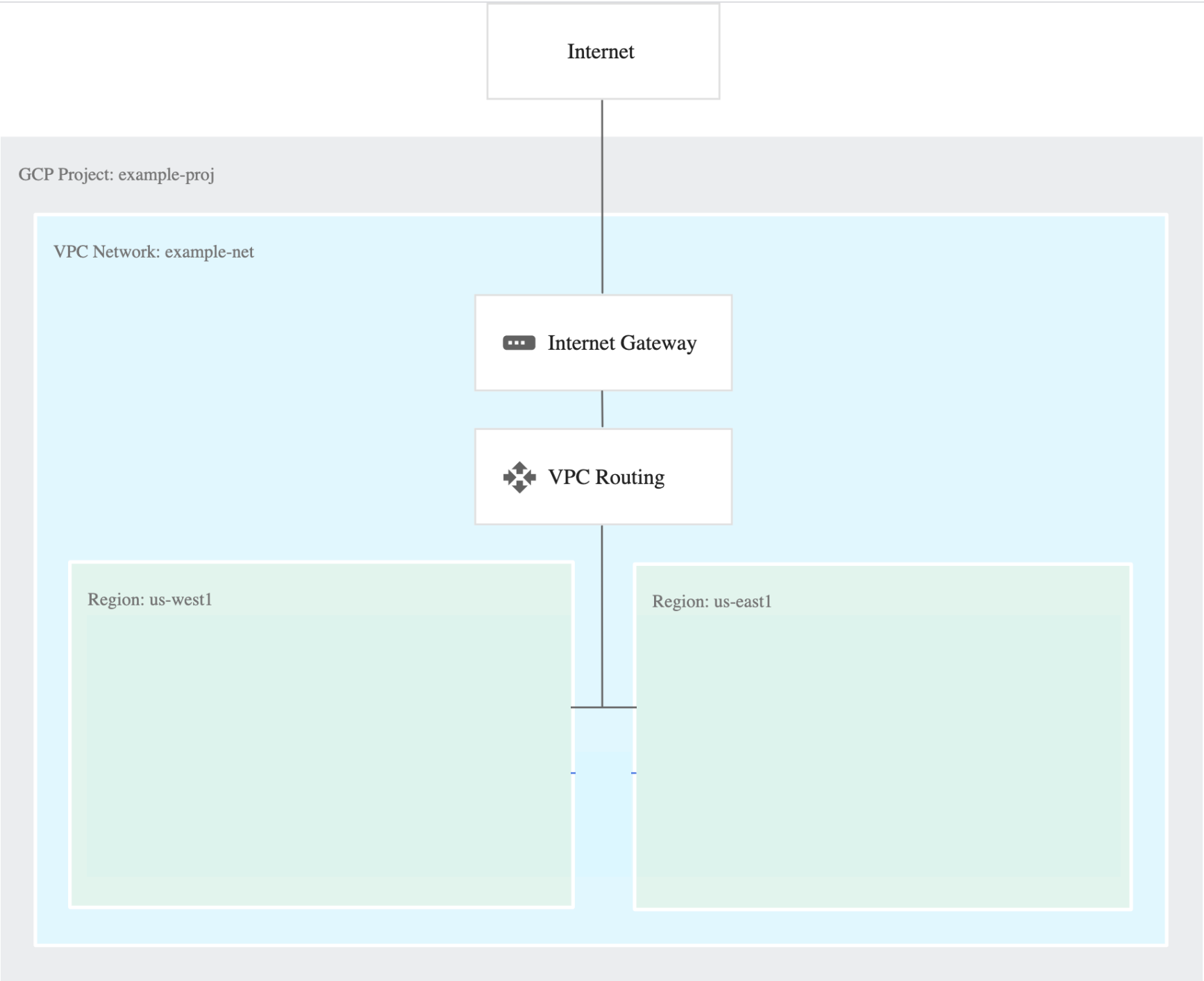
aviatrix

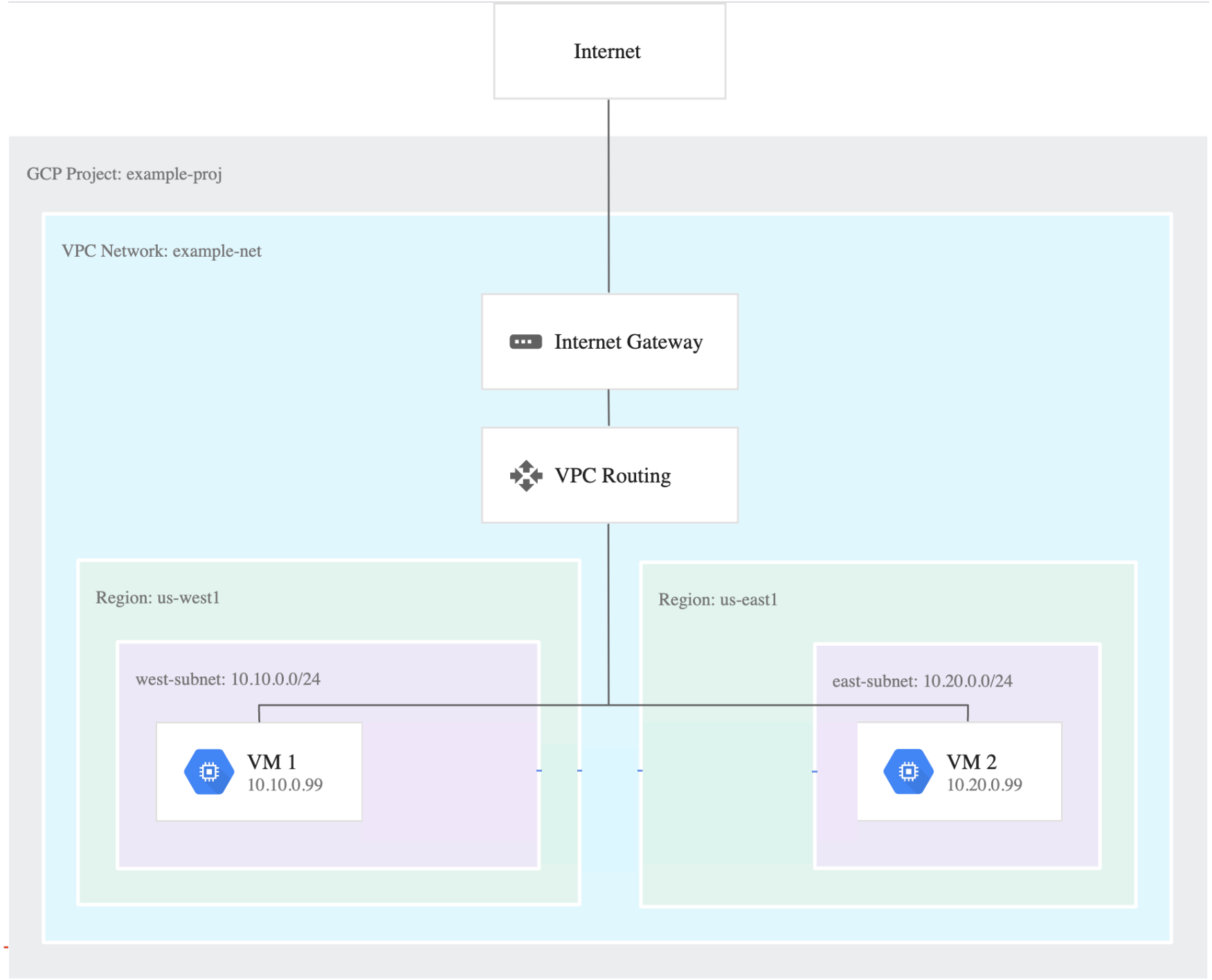
GCP Important Services/Resources

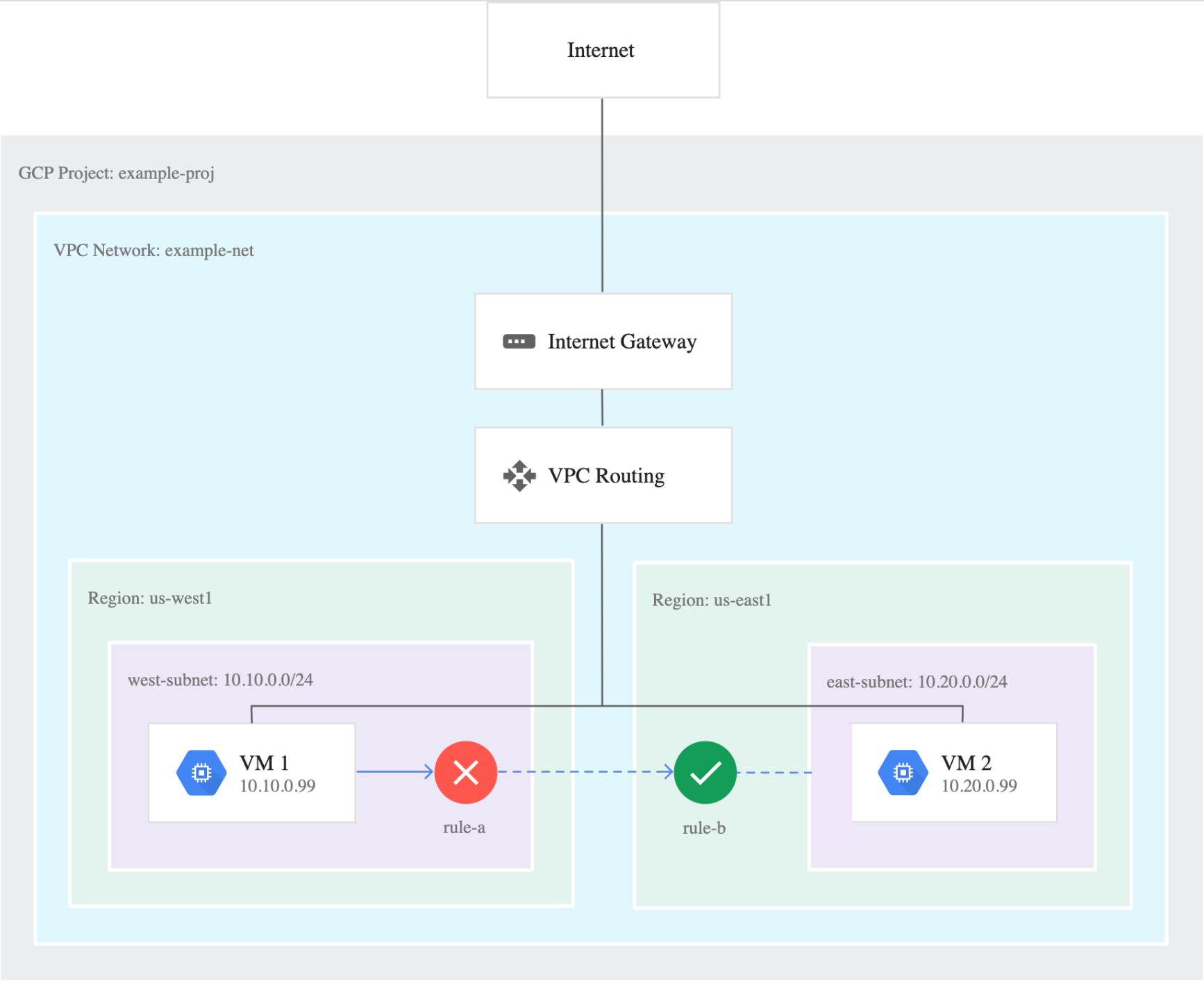
Name	Purpose
Virtual Machine	Run instances (virtual machines)
Cloud IAM	Identity and Access Management
VPC/Subnet	Virtual Private Cloud
Cloud Storage	Storage
Interconnect	Connecting On-Prem
Google Cloud DNS	DNS
Cloud Load Balancing	Leverage close entry points to Cloud Backbone
Cloud CDN	CDN


Internet
GCP Project: example-proj


Internet
GCP Project: example-proj
VPC Network: example-net
Internet Gateway
VPC Routing

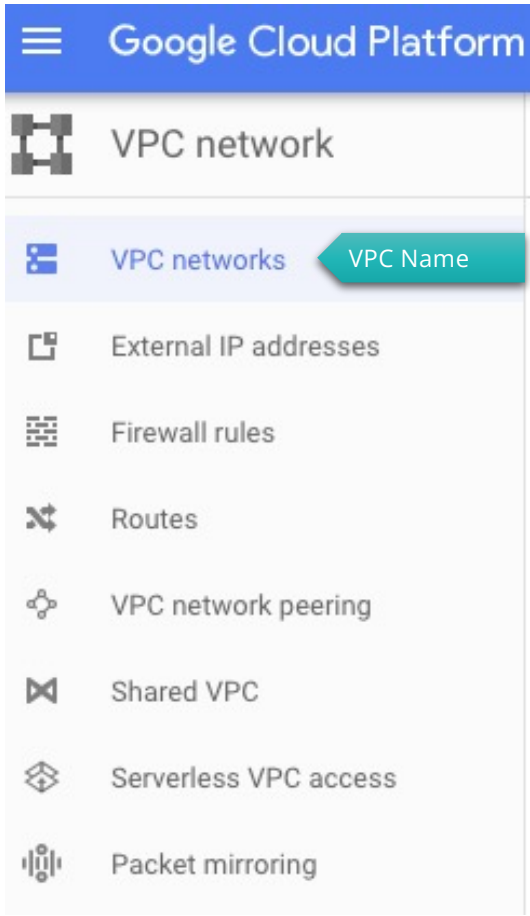

Internet
GCP Project: example-proj
VPC Network: example-net
Internet Gateway
VPC Routing
Region: us-west1
Region: us-east1


Internet
GCP Project: example-proj
VPC Network: example-net
Internet Gateway
VPC Routing
Region: us-west1
west-subnet: 10.10.0.0/24
VM 1
10.10.0.99
Region: us-east1
east-subnet: 10.20.0.0/24
VM 2
10.20.0.99


Internet
GCP Project: example-proj
VPC Network: example-net
Internet Gateway
VPC Routing
Region: us-west1
Region: us-east1
west-subnet: 10.10.0.0/24
east-subnet: 10.20.0.0/24
VM 1
10.10.0.99
rule-a
rule-b
VM 2
10.20.0.99

VPC Network and Subnets

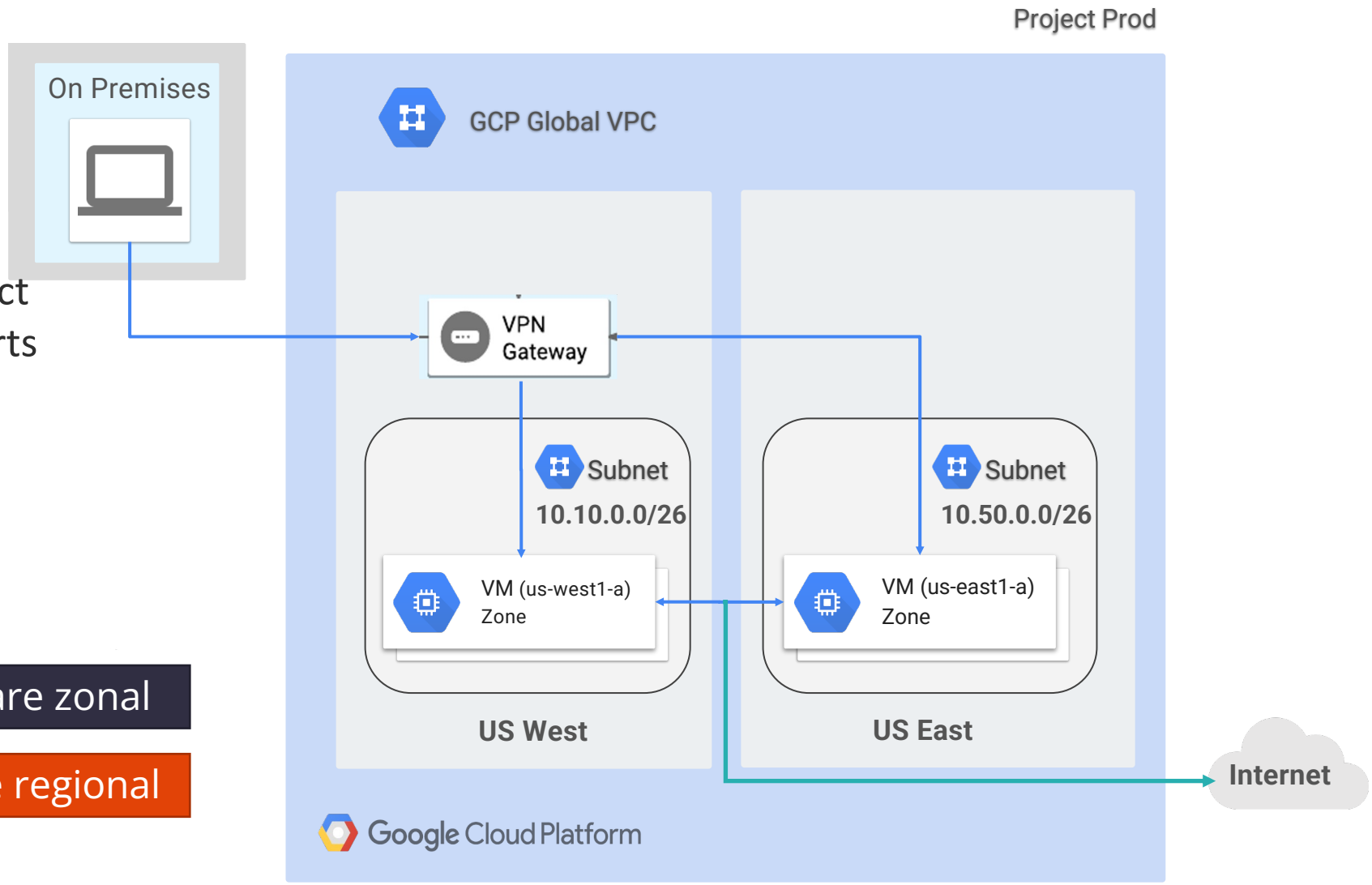
- VPC networks don't have a top level CIDR associated with them (IP ranges are defined at subnet level)
- VPC networks consist of one or more subnets
- VPC Subnets can be created in
  1. Auto Mode (creates subnets in each region automatically)
  2. Custom Mode (VPC networks start with no subnets)
     - You can create more than one subnet per region



VPC Name	Region	Subnets	Mode	IP address ranges	Gateways	Firewall Rules	Global dynamic routing
vpc-network2	asia-east2	vpc-network2-subnet1	Custom	10.39.39.0/24	10.39.39.1	0	On
Default	us-central1	Default	Auto	10.128.0.0/20	10.128.0.1	6	Off

Basic GCP Networking Components

- GCP Regions and Zones
- VPC /Subnets
- VPC Peering
- Implicit Routing
- VPN Gateway: Used to connect to your on-prem. Only supports BGP
- VPCs can be peered
    - Not transitive
    - Requires full mesh



In AWS: VPC is regional, subnets are zonal

In GCP: VPC is global, subnets are regional

GCP VPC Design Best Practices

- Create multiple region-bound VPCs
  - For proper segmentation
  - Encryption
  - Service Insertion

- The Aviatrix transit combined with regional VPCs is the recommended approach

Solutions Products Pricing Getting St English Console

Contact Us Get started for free

Create a VPC network for each autonomous team, with shared services in a common VPC network

Some large enterprise deployments involve autonomous teams that each require full control over their respective VPC networks. You can meet this requirement by creating a VPC network for each business unit, with shared services in a common VPC network (for example, analytic tools, CI/CD pipeline and build machines, DNS/Directory services). For more information about creating a common VPC network for shared services, see the shared services section.

Source: https://cloud.google.com/solutions/best-practices-vpc-design

Solutions Products Pricing Getting Star Docs Support English Console

Contact Us Get started for free

Start with a single VPC network for resources that have common requirements

For many simple use cases, a single VPC network provides the features that you need, while being easier to create, maintain, and understand than the more complex alternatives. By grouping resources with common requirements and characteristics into a single VPC network, you begin to establish the VPC network border as the perimeter for potential issues.

For an example of this configuration, see the single project, single VPC network reference architecture.

Factors that might lead you to create additional VPC networks include scale, network security, financial considerations, operational requirements, and identity and access management (IAM).

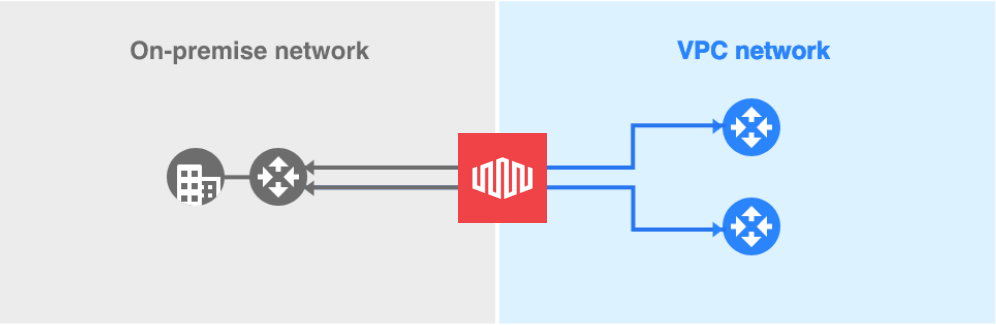
Cloud Interconnect

- Connect on-prem network to VPC network through a private circuit
- Two types of Cloud Interconnect
  1. Dedicated Interconnect
     - Meet GCP network in a colocation facility
     - 10 Gbps or 100 Gbps pipes
  2. Partner Interconnect
     - Connect to service providers that connect directly to Google
     - 50 Mbps to 50 Gbps
     - Layer 2 or Layer 3 connections are supported
- Both support multiple VLAN attachments for redundancy
- **Encryption limited to 1.25 Gbps without Aviatrix**

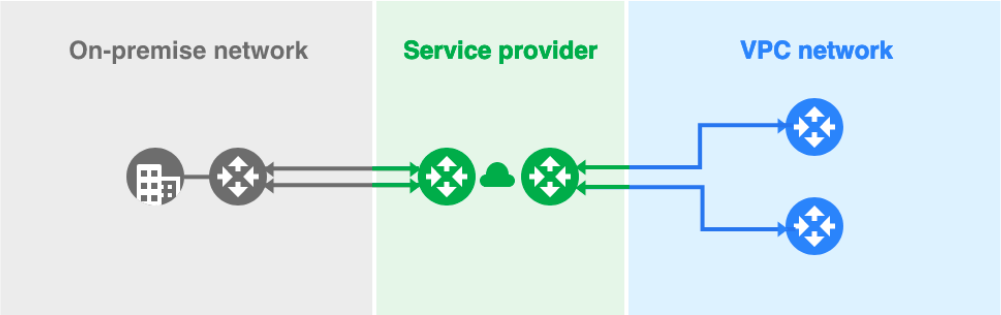
Choose an interconnect type that fits your networking needs:

Interconnect type

Dedicated Interconnect Connect your on-premises network to your Google Cloud VPC network by connecting a new fiber to your equipment. Learn more

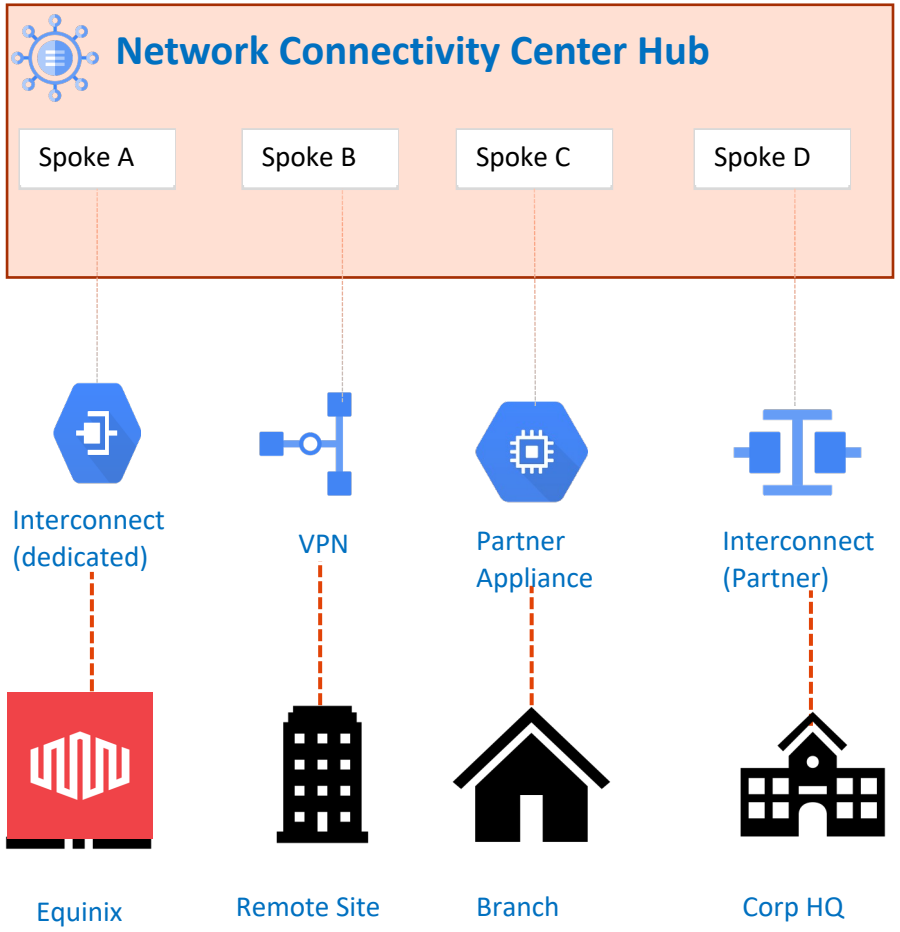


Partner Interconnect Connect your on-premises network to your Google Cloud VPC network through a connection from a supported service provider. Learn more or check supported service providers



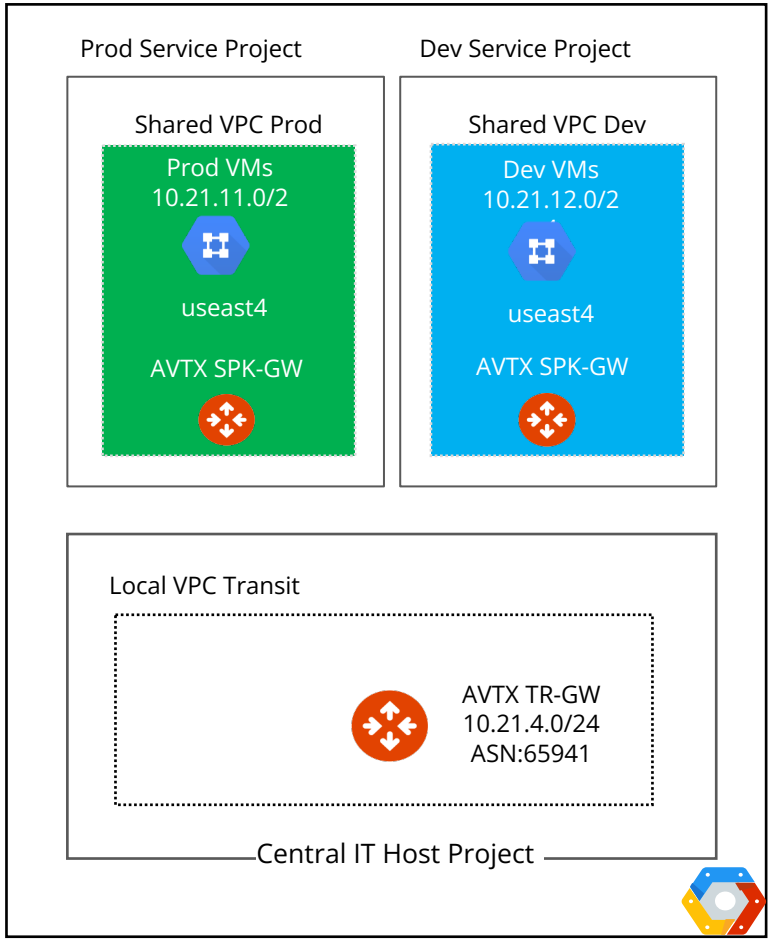
Network Connectivity Center (NCC)

- **What is it?**
  - A hub and spoke model where the hub is a Google construct consisting of at least one cloud router and spokes
  - Spokes can be Cloud Interconnect circuits, Cloud VPN connections or third-party virtual instances (called Router Appliances)
- **Limitations**
  - The same VPC network must connect all spokes to the hub
  - No multi-cloud support



GCP Shared VPC

- Use case
  - Centralize the control of network resources like subnets, routes, and firewalls.
  - Improve the security by restricting network resource control to only network teams.
- A Shared VPC is a VPC defined in a host project
- A shared VPC network is shared in a service project (tenant project)
  - Technique for providing networking services to tenant VPCs
- A Service Project is a project that has been attached to a host project
  - A Shared VPC Admin gives its VPC or subnet to the Service Project
- All VPCs must be in the same organization
- Each service project can only be attached to a single host project
- Shared VPC is not a transit replacement
- Shared VPC has no Control Plane or Data Plane → IAM construct
- "Shared VPC" is not equal to "Shared Services VPC"
  - It is not necessarily meant to be hosting shared services in the shared VPC



Next: OCI Networking 101