Architecting Global Private Clouds with VPC Networks

UNDERSTANDING VPC NETWORKS ON THE GCP

Janani Ravi
CO-FOUNDER, LOONYCORN

www.loonycorn.com

Overview

VPCs are isolated, private partitions for resources

Contain abstractions for routes, rules and IP addresses

VPCs are global, span regions

Composed of regional subnets

Auto mode and custom mode VPCs

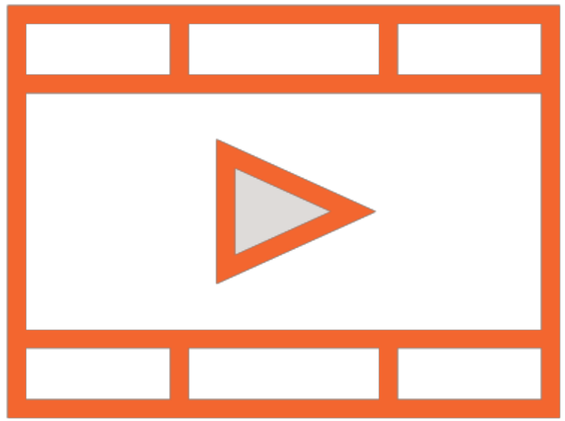
Prerequisites and Course Outline

Software and Skills

Basic understanding of cloud computing

Basic understanding of how virtual machines work

Basic understanding of networking concepts



Prerequisites: Basic Cloud Computing and Networking

Choosing and Implementing Google Cloud Compute Engine Solutions

- Basics of using the Google Cloud Platform

Networking Concepts and Protocols

- Fundamentals of data networking

Course Outline

Introducing VPC networks

- Global VPCs, regional subnets
- Auto mode and custom mode networks
- Communication between instances on the same VPC

Working with firewalls

- Components of a firewall rule
- Permissions, direction, priority, filters, protocols, ports
- Using network tags

Leveraging shared VPCs

- Sharing VPCs across projects
- Host project, service projects

Scenarios: SpikeySales.com

Hypothetical online retailer

- Flash sales of trending products
- Spikes in user traffic

SpikeySales on the GCP

- Cloud computing fits perfectly
- Pay-as-you-go
- No idle capacity during off-sale periods
- Elastic, pay-as-you-go, global access

VPCs and Networking on the Google Cloud

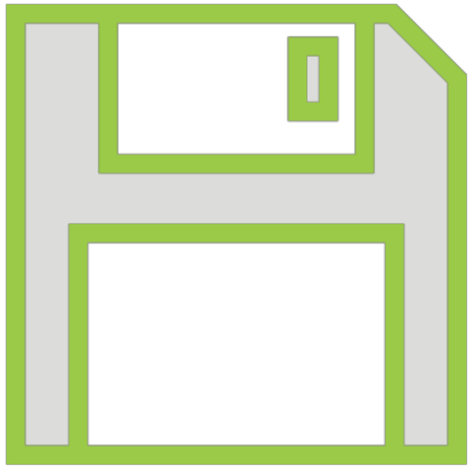
Cloud Computing

The practice of using a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or a personal computer.

Choices in (Any) Computing

Compute

Where and how does code run?



Storage

Where and how is the data stored?

Once you've figured these out, move on to other choices - networking, logging, monitoring

Networking Must-haves

Objective	GCP Solution
Resources within a project need to communicate	Internal IP addresses
Resources on GCP need to communicate with outside world	External IP addresses
Traffic sent to an IP address needs to reach that address	Routes
Platform users need to be able to restrict traffic flows	Firewall rules

Networking Must-haves

Objective	GCP Solution
Resources within a project need to communicate	Internal IP addresses
Resources on GCP need to communicate with outside world	External IP addresses
Traffic sent to an IP address needs to reach that address	Routes
Platform users need to be able to restrict traffic flows	Firewall rules

IP addresses, routes and firewall rules all exist inside a GCP resource called a VPC Network

VPCs and Subnets

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

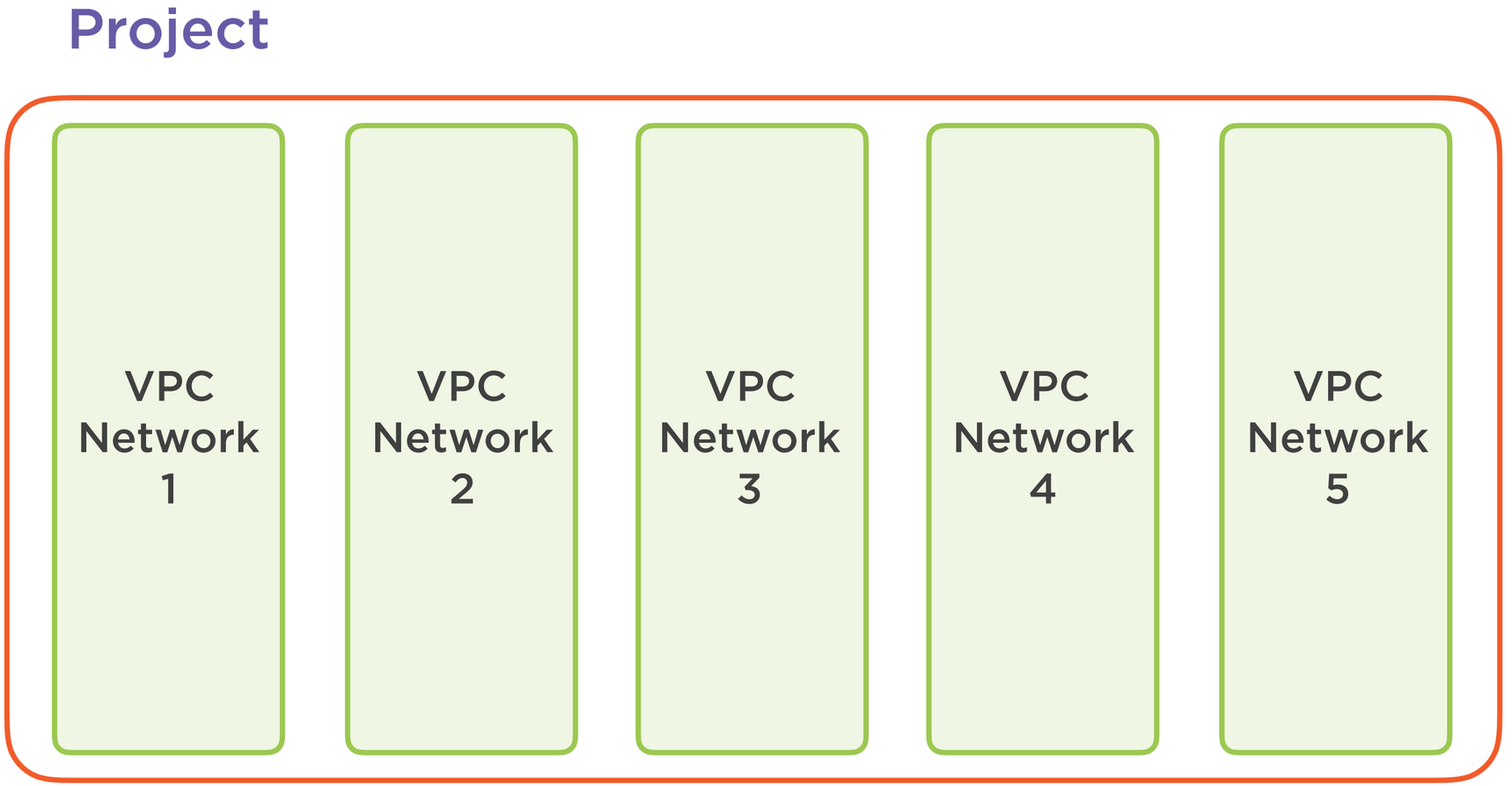
▸“Virtual Private Cloud”

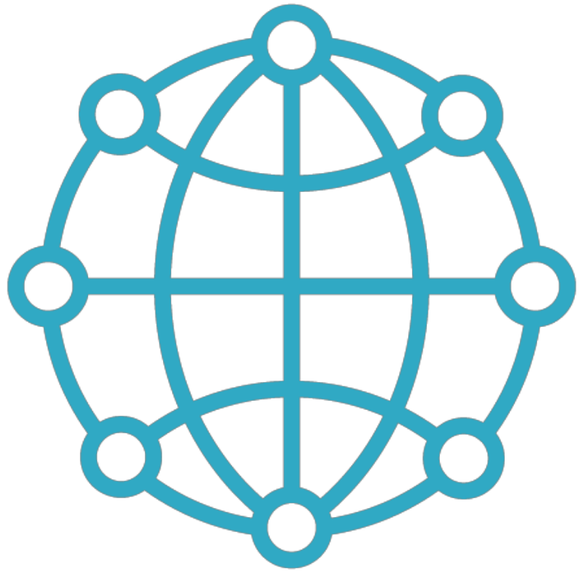
Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

- Every VPC is a resource and must exist inside a project

Multiple VPCs in a Project





Projects and VPCs

VPCs are GCP resources

Each VPC must exist inside a project

Default VPC pre-created in each project

Can add additional VPCs

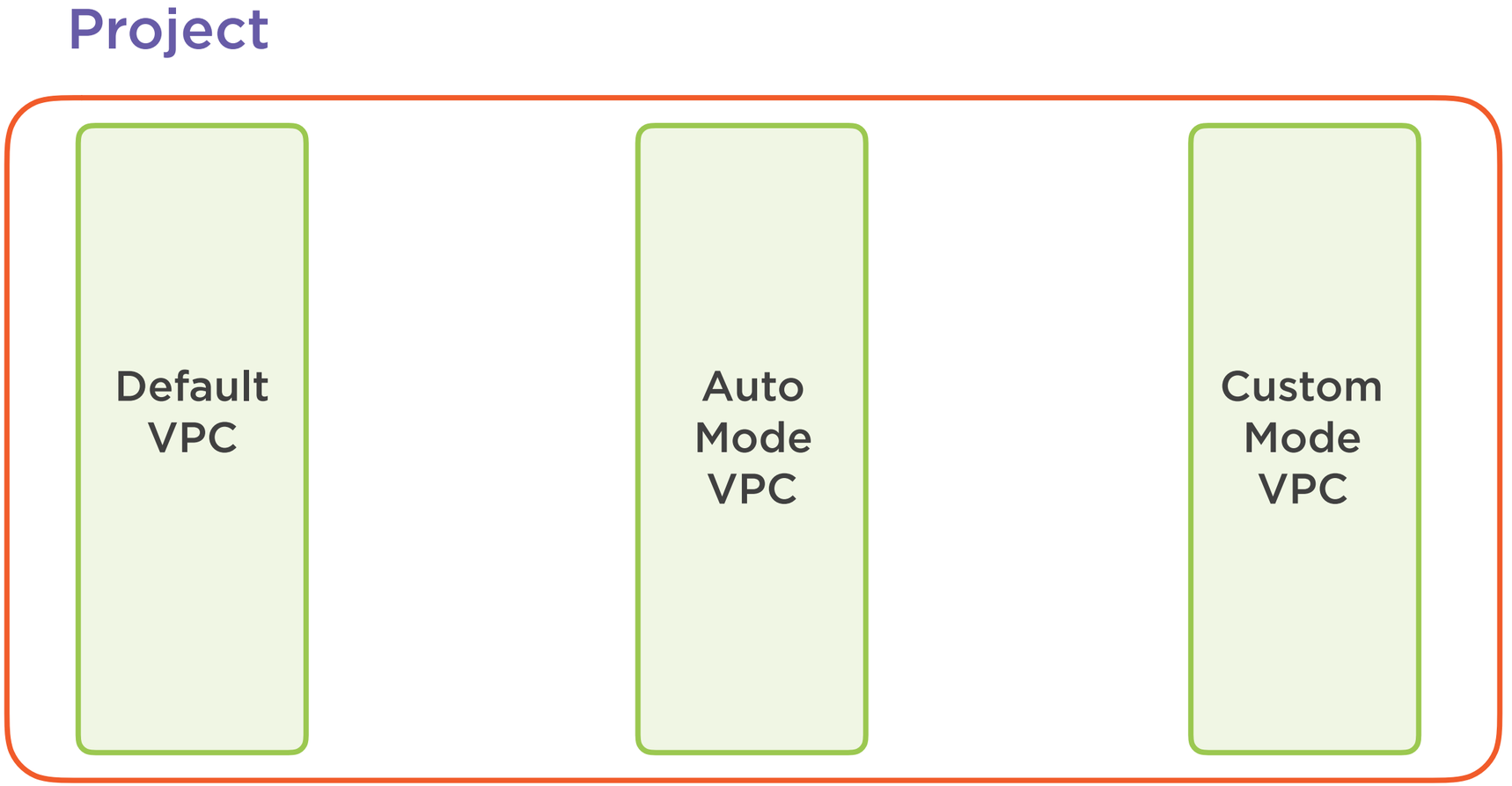
- Auto Mode
- Custom Mode

VPC is a term also used on AWS, with similar but subtly different meaning - just saying “network” usually means AWS

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Custom Mode and Auto Mode

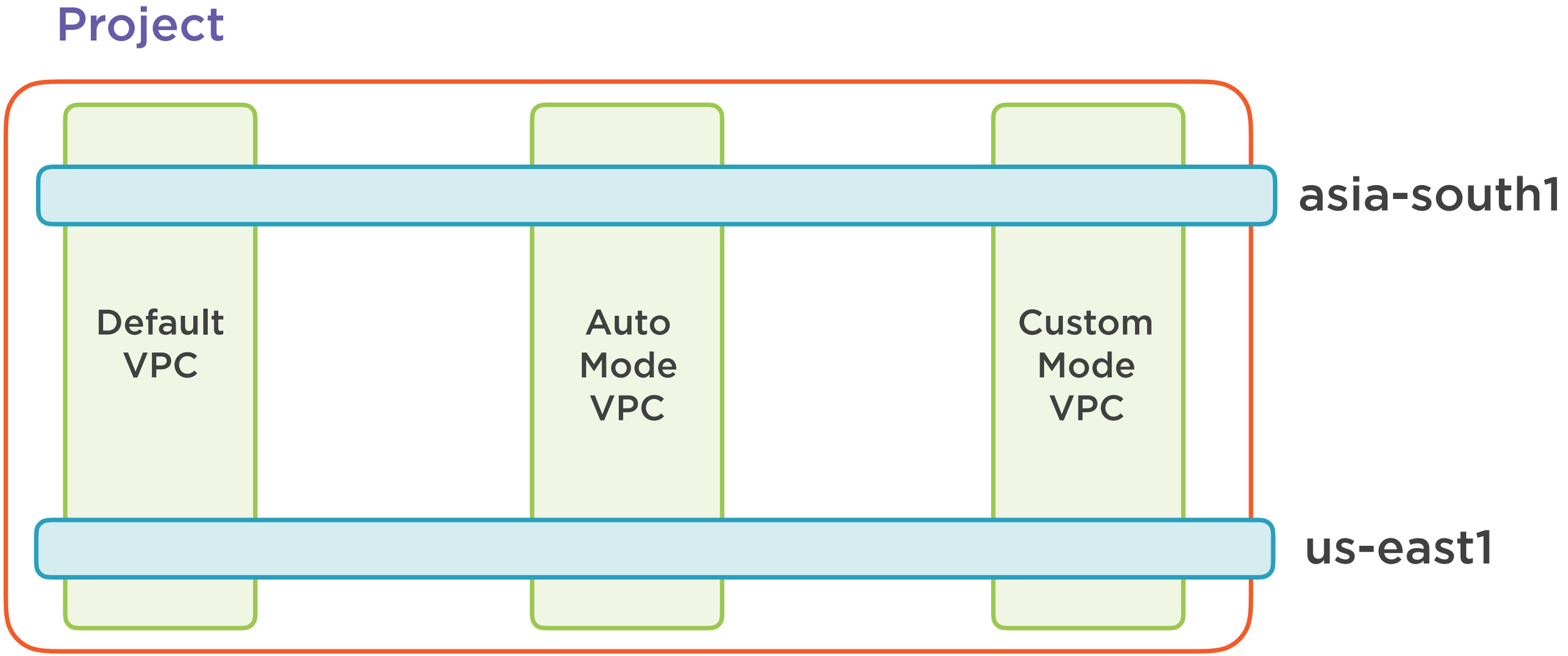


Can have resources in different regions on the same VPC

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

VPCs Are Global

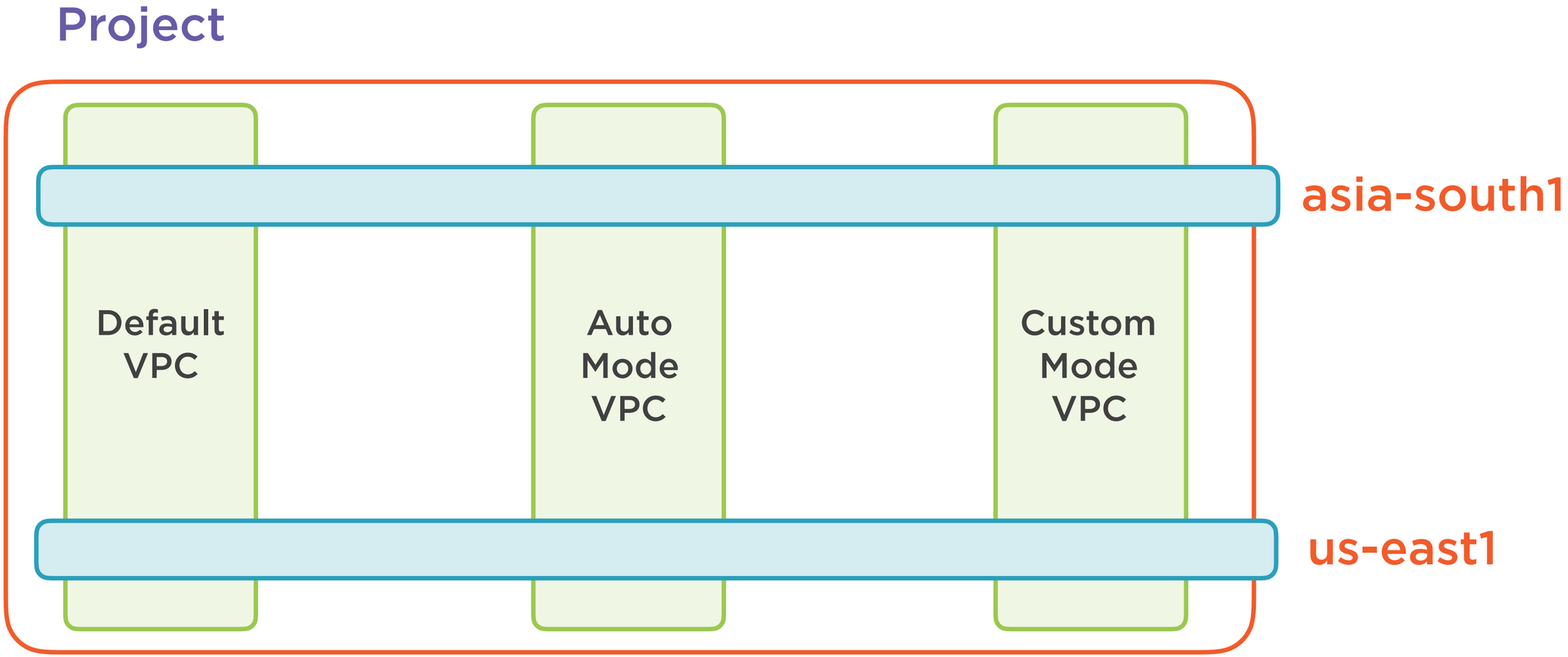


Google VPCs span regions (AWS VPCs are regional)

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

VPCs Span Regions



VPCs include subnets; each subnet is regional

Google VPC a.k.a. “Network”

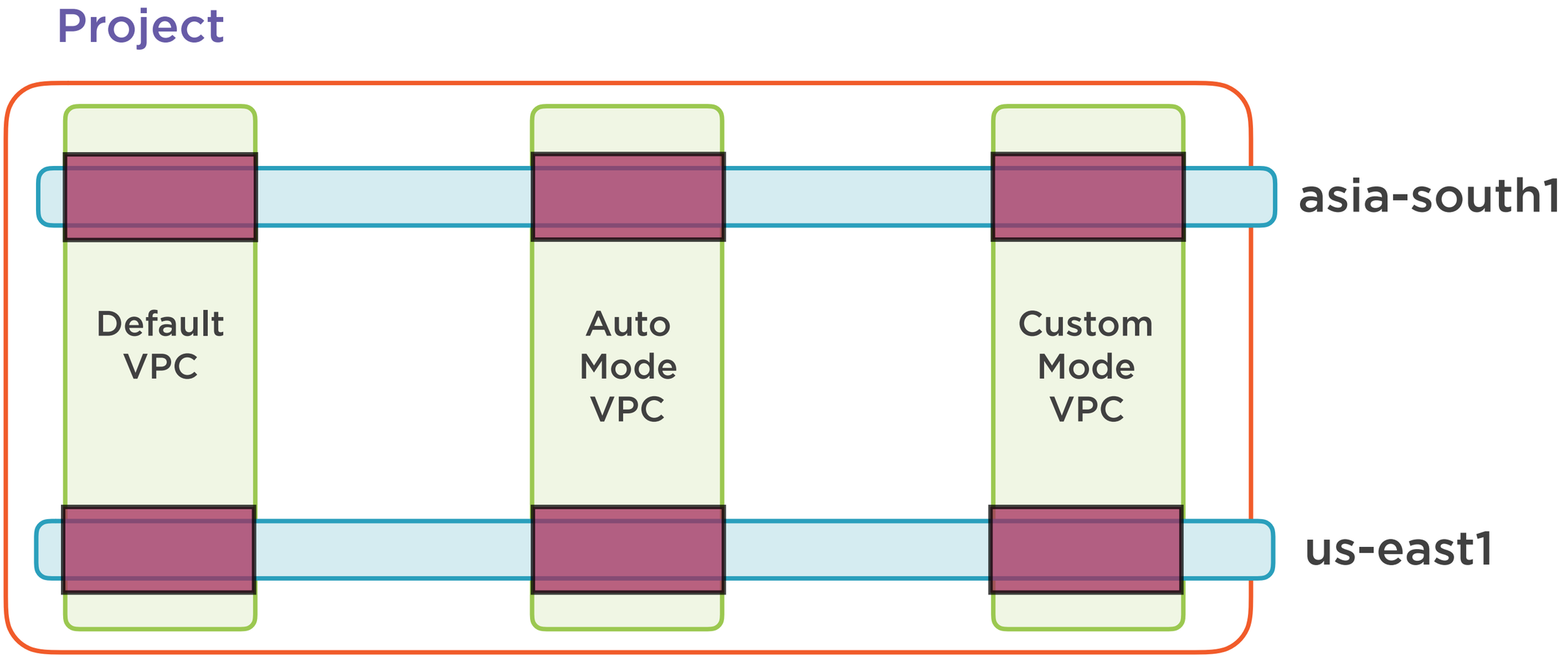
A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Google VPC a.k.a. “Network”

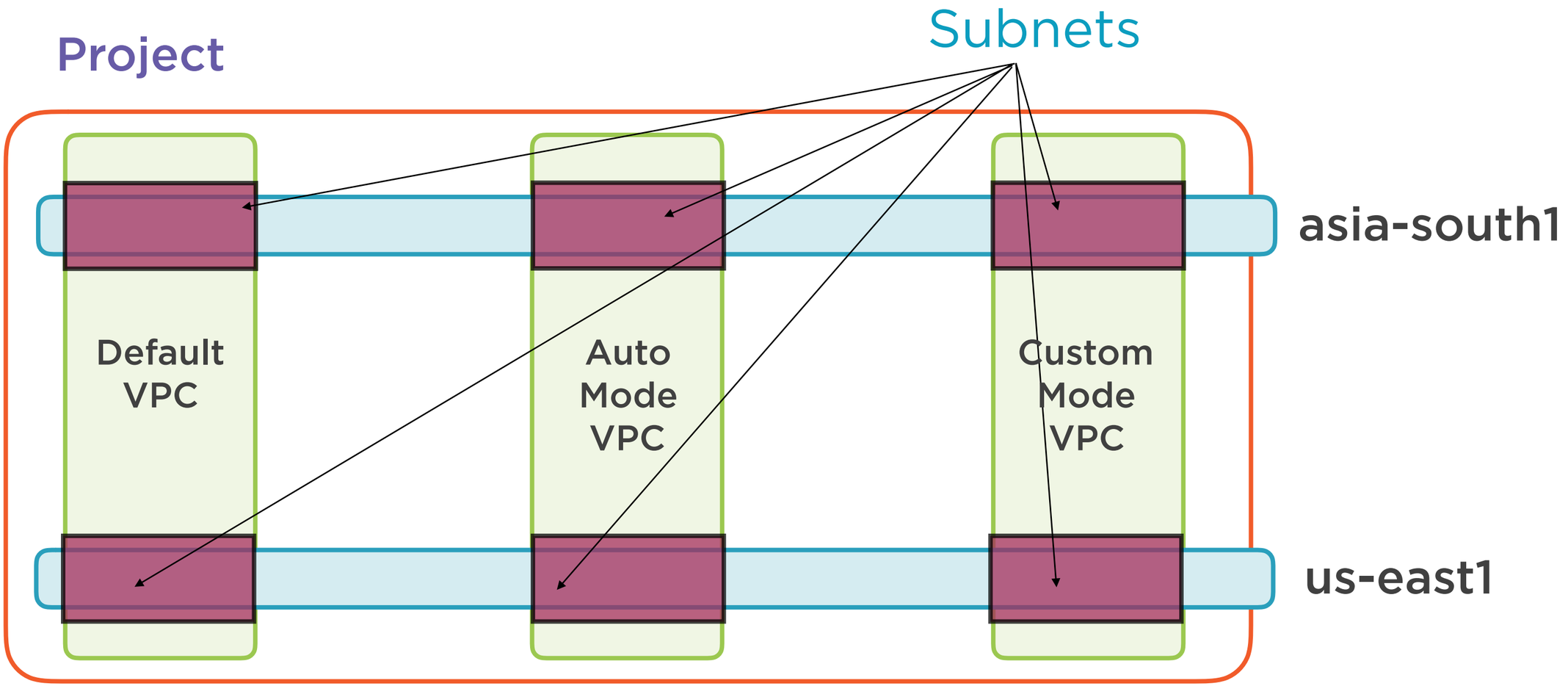
A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Any resource on a VPC must exist on some subnet

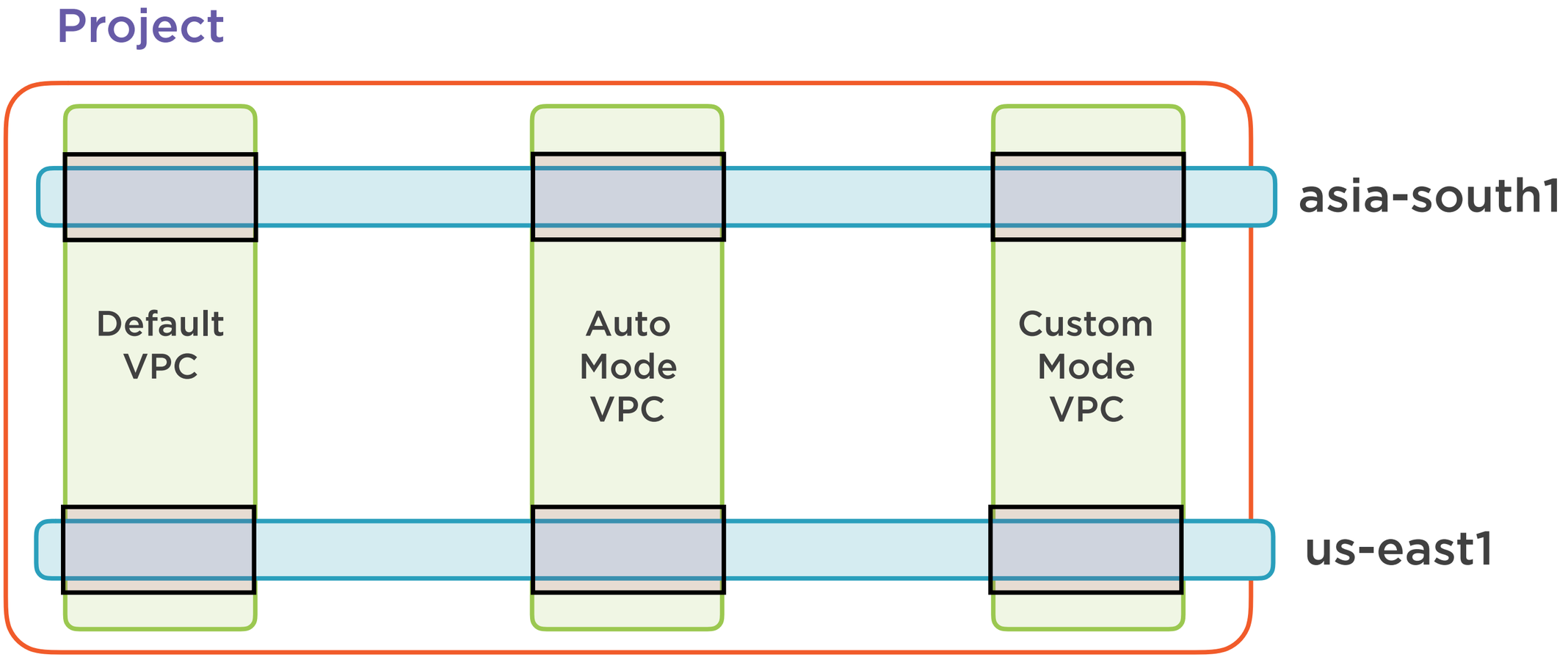
Subnets in Each Region



Subnets in Each Region

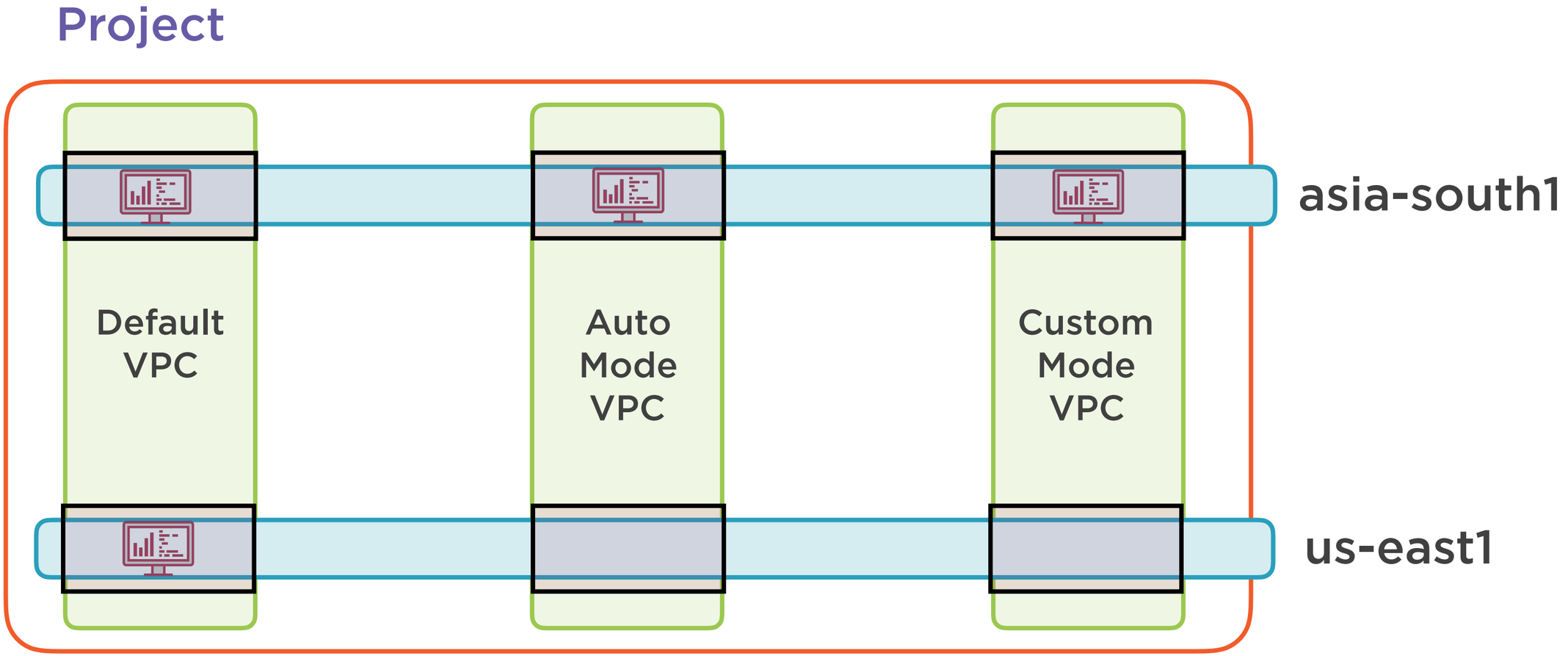


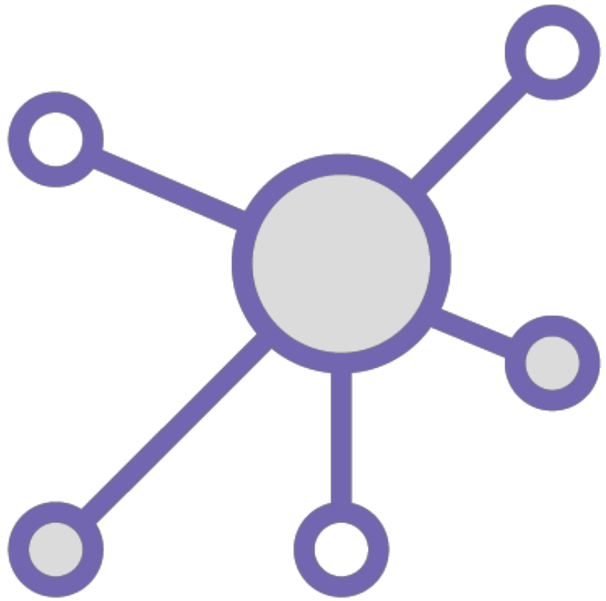
Subnets to Group and Manage Resources



GCP subnets need not fit into a larger address hierarchy

Resources Provisioned on Subnets





Subnets

VPC networks are global

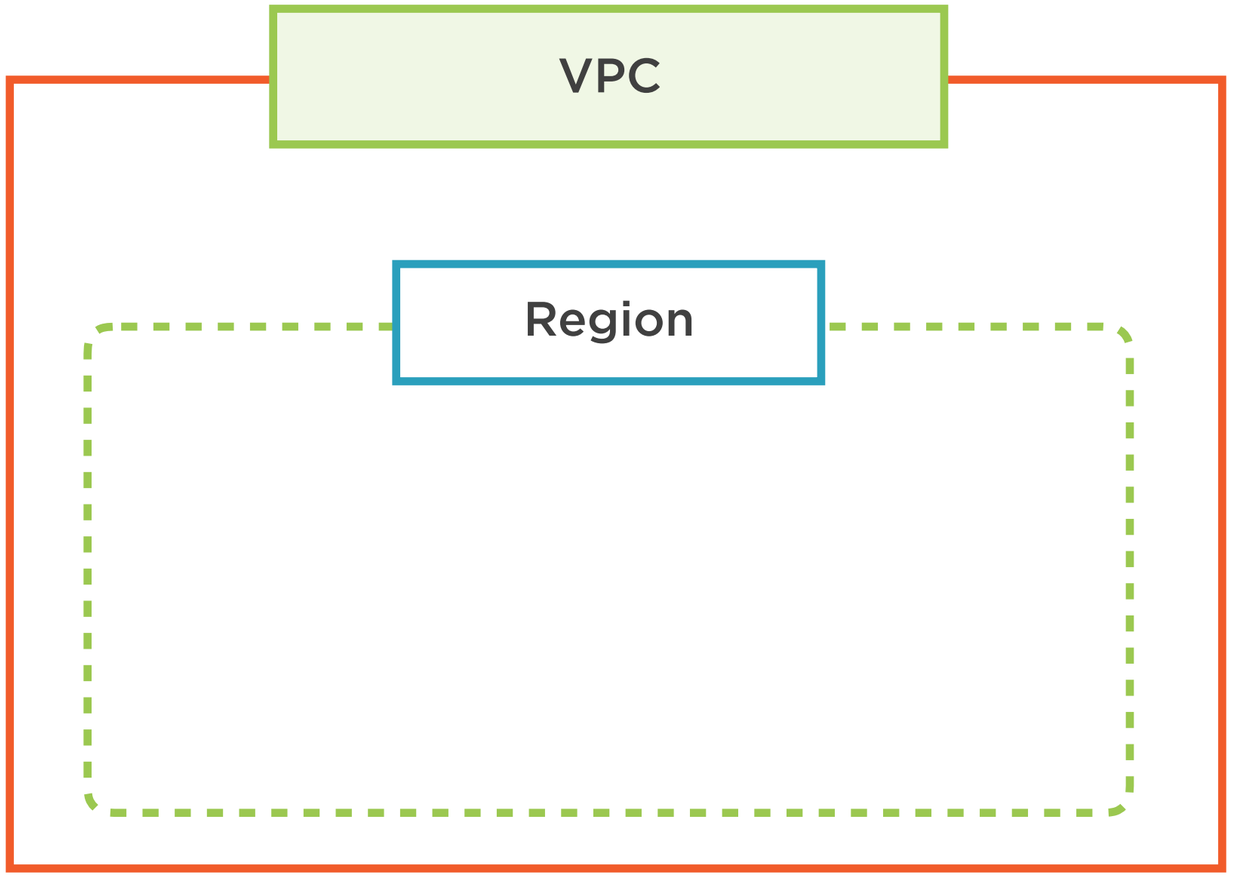
Subnets are regional

(Can span zones inside a region)

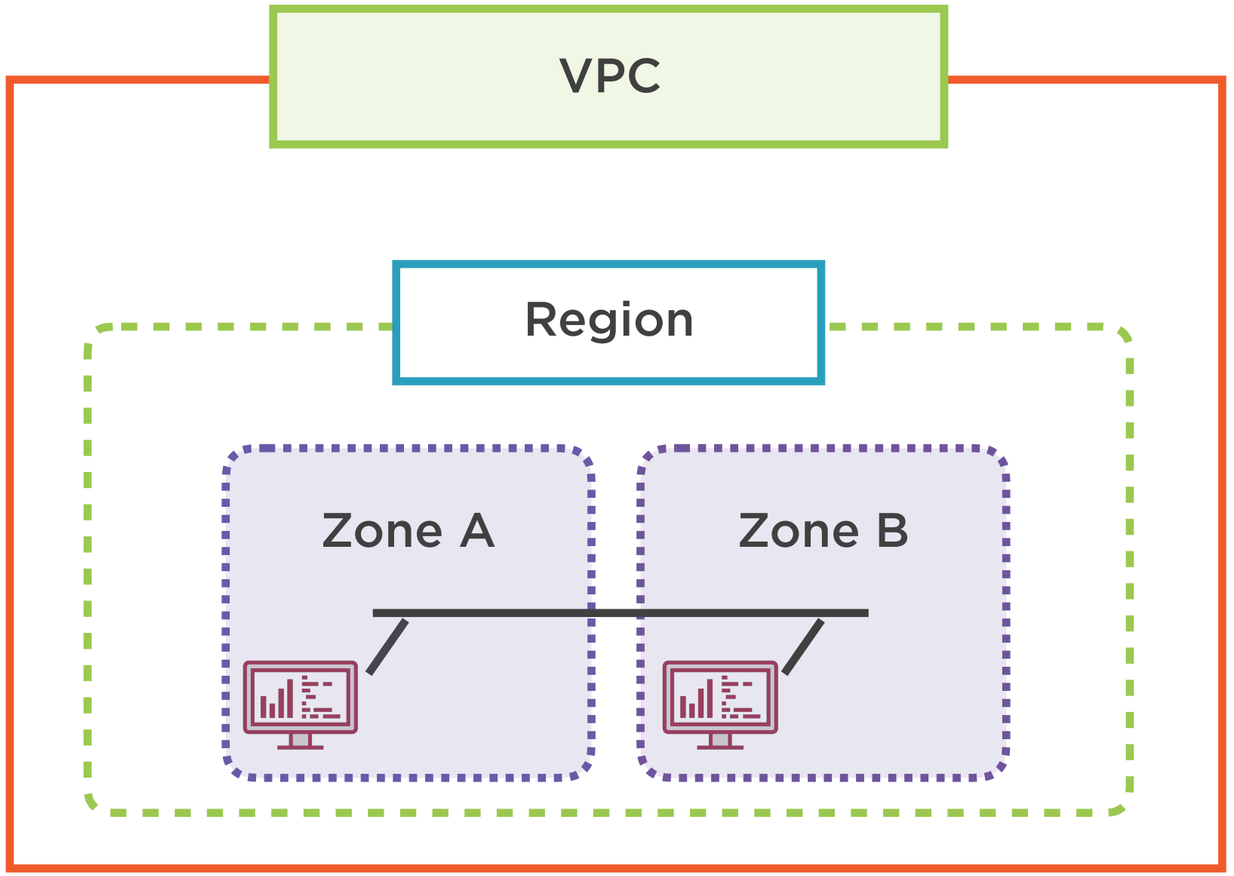
Every VPC consists of subnets

Auto Mode VPCs have pre-created subnets

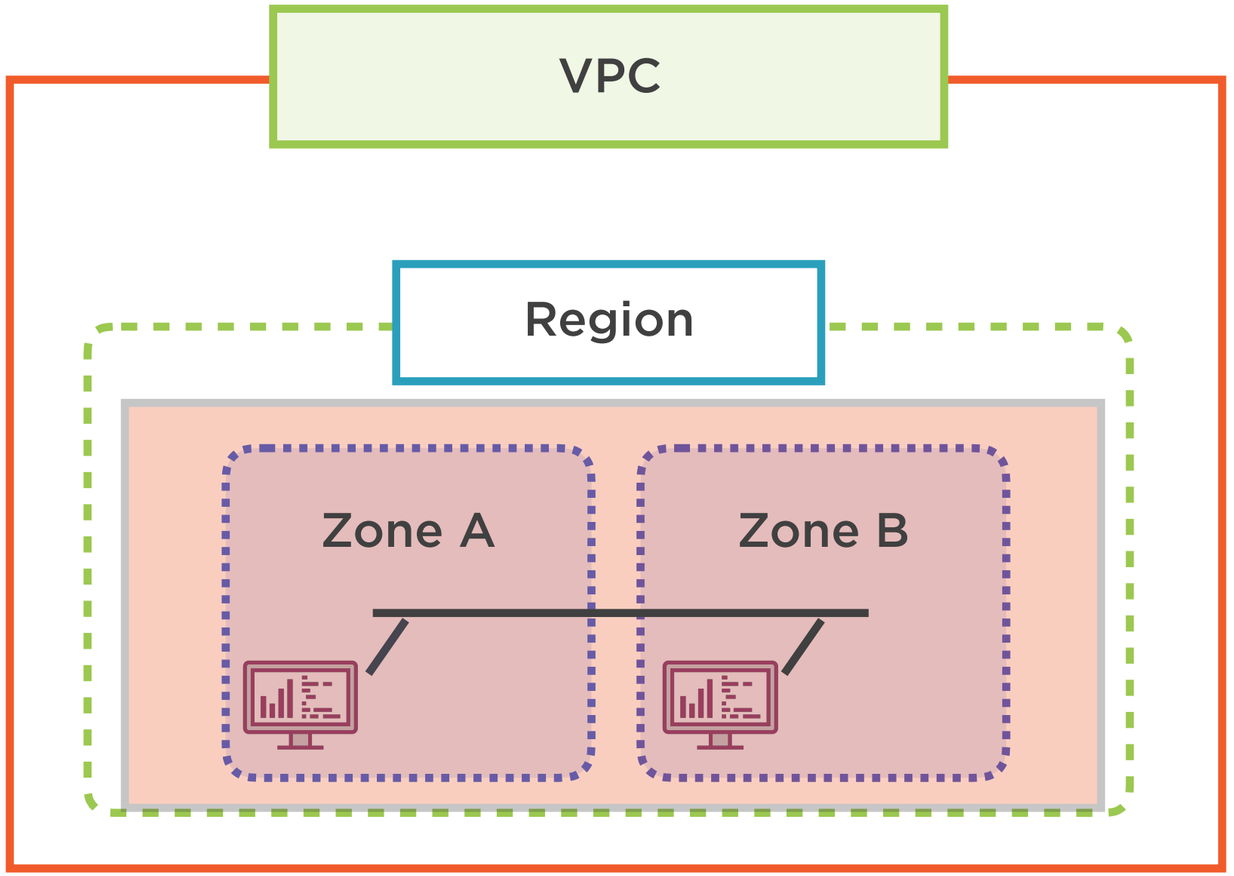
Subnets Span Zones

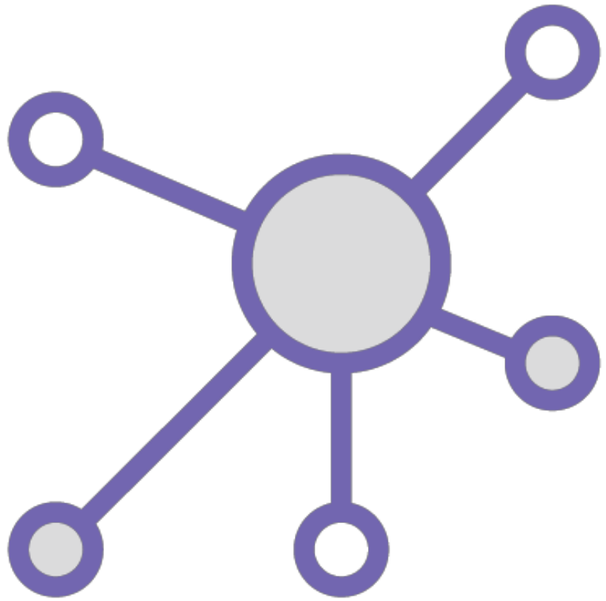


Subnets Span Zones



Subnets Span Zones





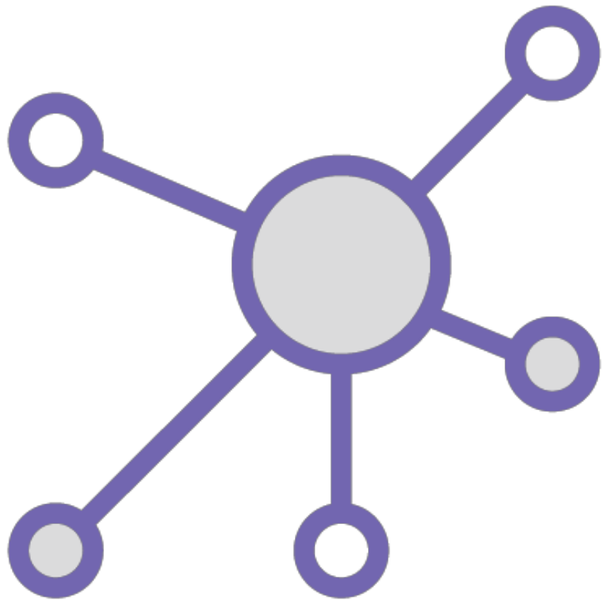
Subnets and IP Ranges

Each subnet must have primary address range

Valid RFC 1918 CIDR block

Subnet ranges in same network cannot overlap

Subnet ranges in different networks can overlap



Reserved IPs

Every subnet has four reserved IP addresses

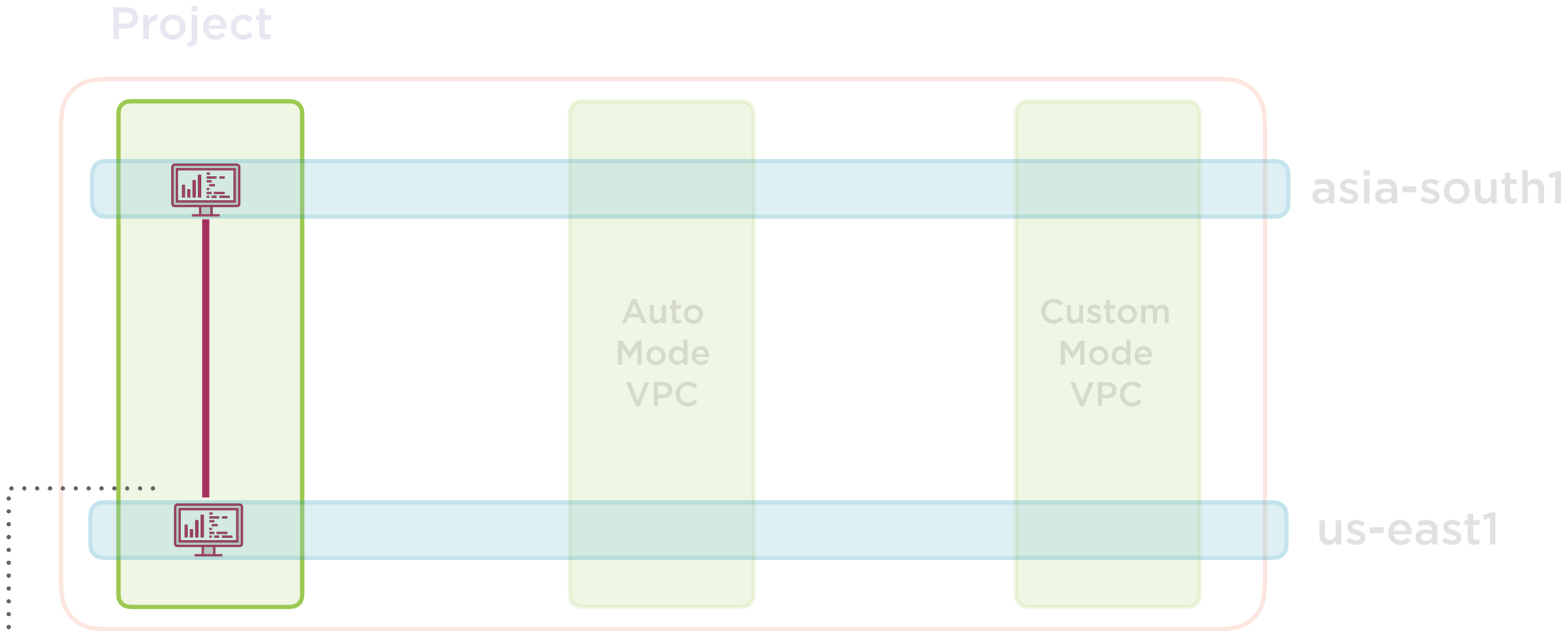
- Network
- Default Gateway
- Second-to-last Reservation
- Broadcast

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

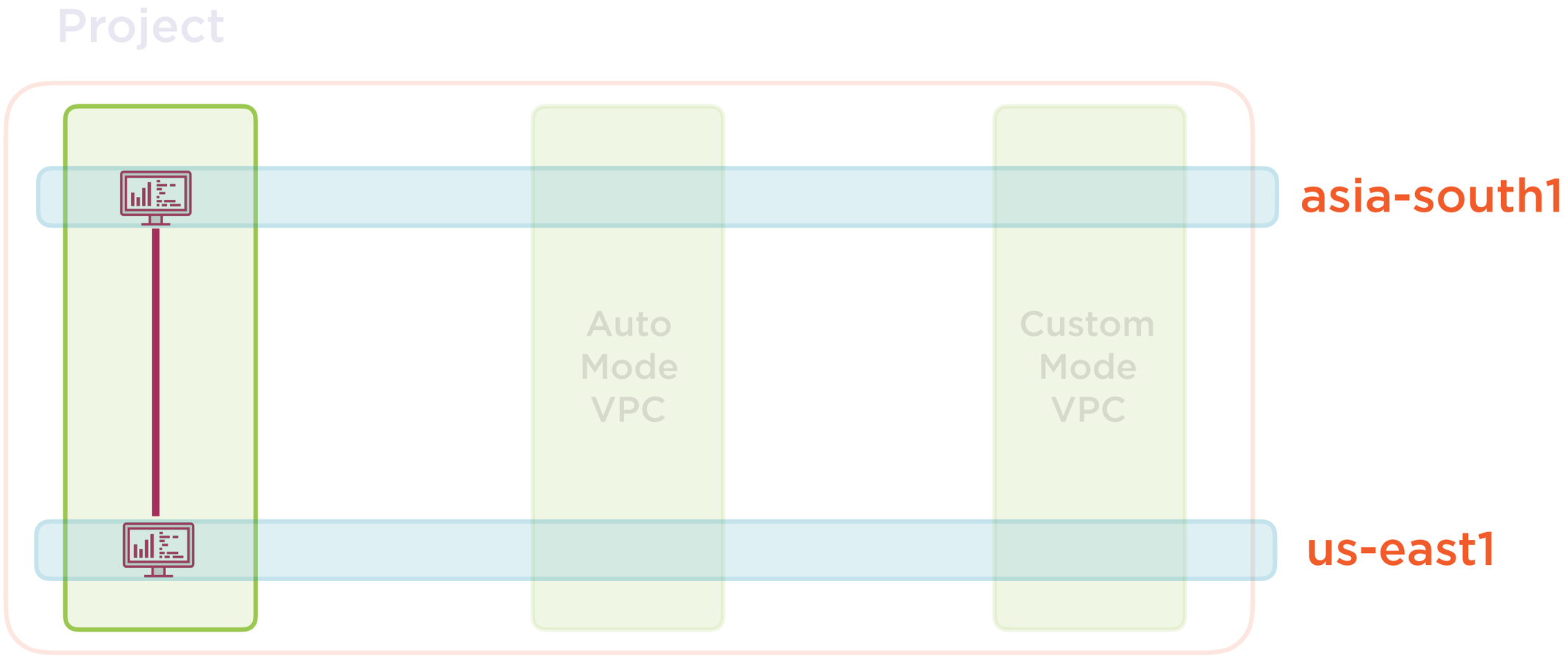
Resources within VPC communicate using private IP addresses

Communication on VPCs



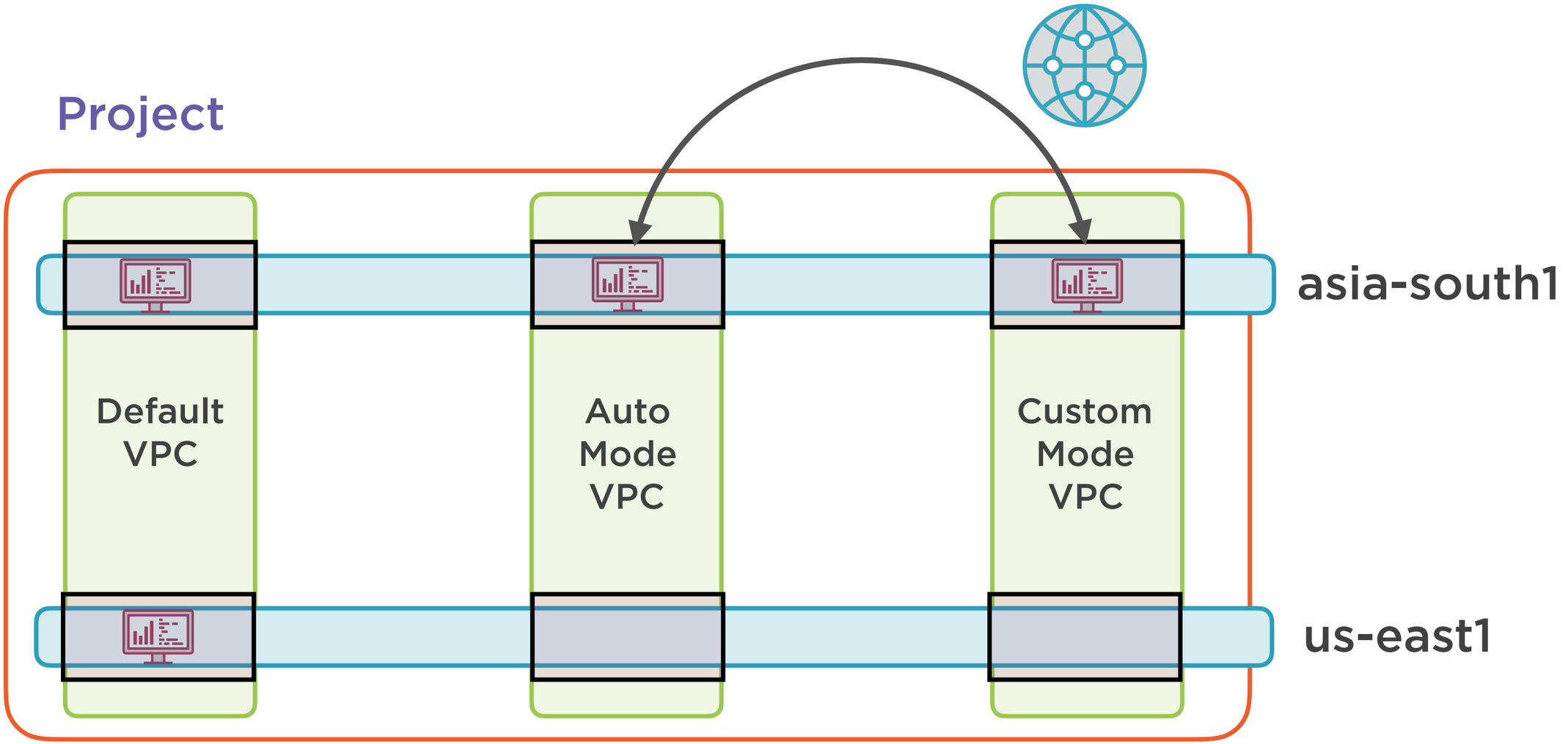
Resources within VPC communicate using private IP addresses

Communication on VPCs



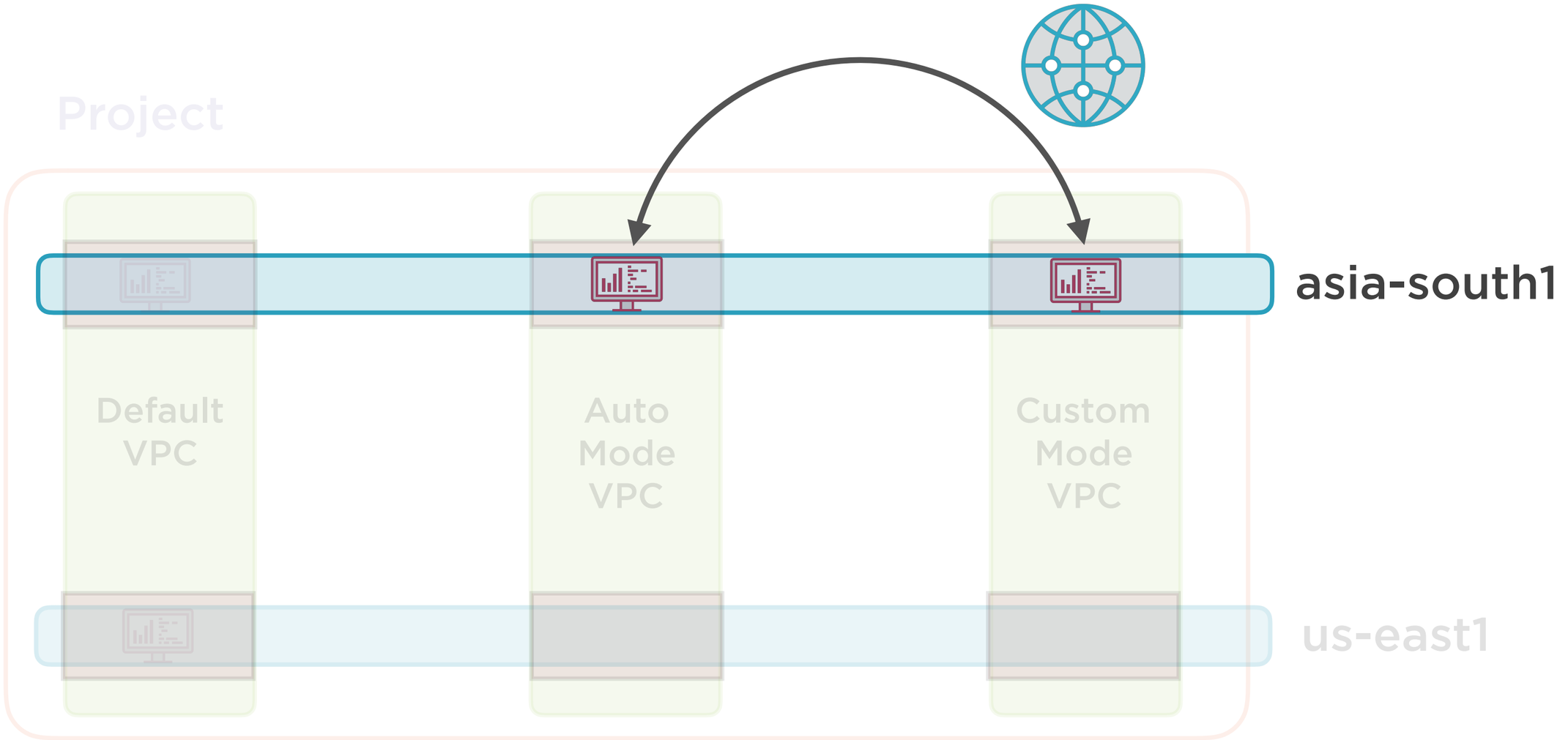
Physical location does not matter

Communication on VPCs



Resources on different VPCs communicate over the internet using external IPs

Communication on VPCs



Even though they are in the same region

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

- Firewall rules restrict and regulate network traffic flows in a VPC

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Under the hood, Google is routing traffic - that’s how VPCs can be global

Google VPC a.k.a. “Network”

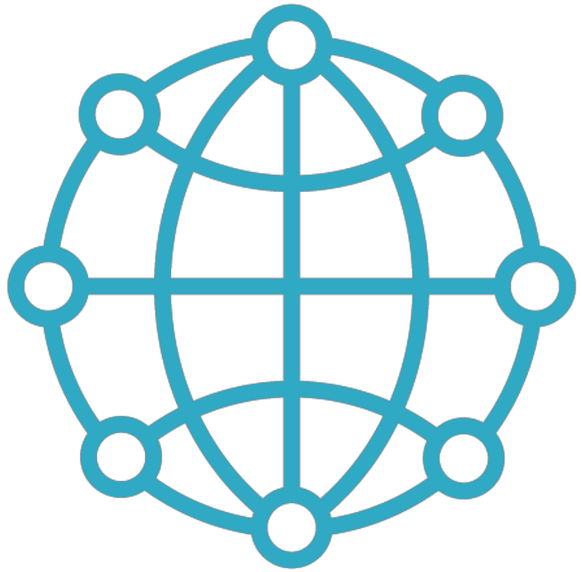
A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Routes, firewall rules, tags, IP addresses are all managed by the platform

Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Default VPC



VPCs

VPCs are global

Governed by IAM roles

Shared VPC: Host project, guest resources

VPC Peering: Intra-GCP communication

Interconnecting VPCs

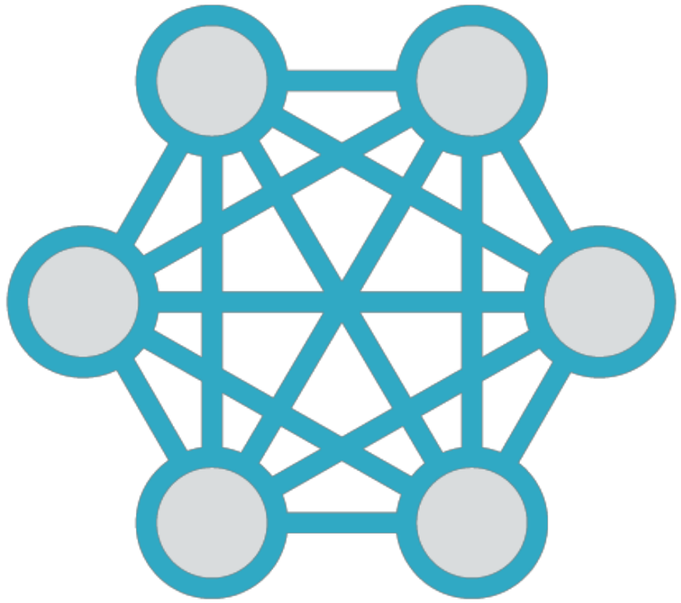
Can work in hybrid environments

- Cloud VPN
- Cloud Interconnect
- Peering

Covered in separate course

Networking Must-haves

Objective	GCP Solution
Users should not have to deal with networking if they don't want to	Default VPC
Users should be able to separate resources even within a project	Additional VPCs
Users should be able to control granular details if they really wish to	Custom Mode VPCs



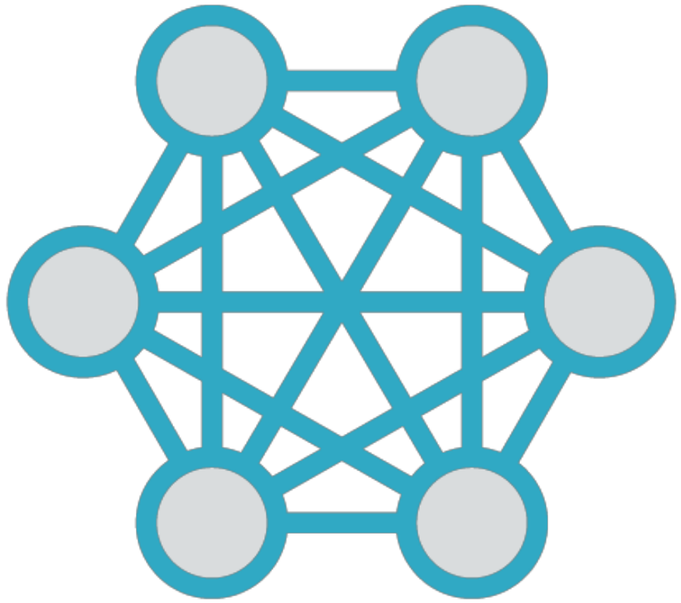
Default VPC

Pre-created on every project

Includes subnet for each GCP region

New subnets added when new regions are created

Resources created here by default



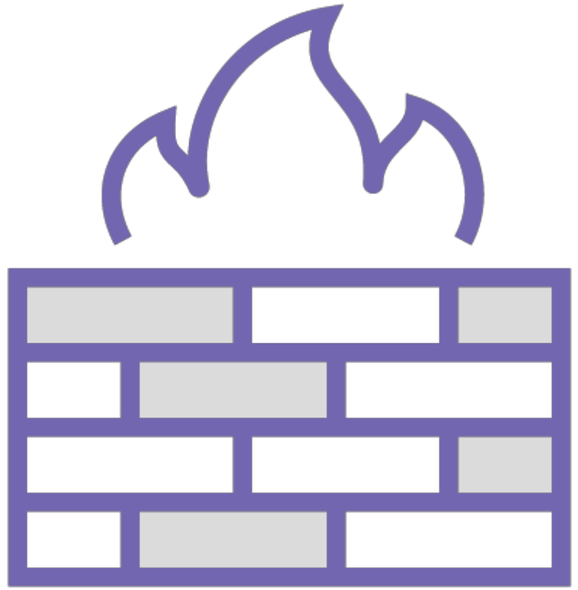
Default VPC

Includes routes for all resources

(This is how VMs can ping each other)

Default gateway to internet

Includes several firewall rules



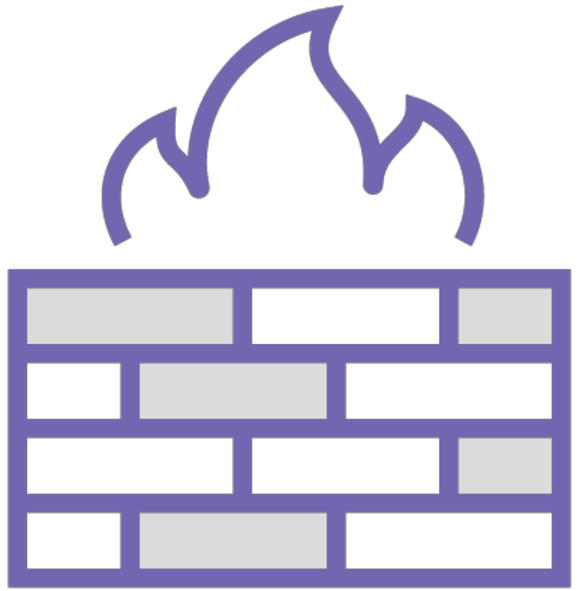
Firewall Rules

Every VPC is a distributed firewall

Firewall rules defined in VPC

Are applied on per-instance basis

Can also regulate internal traffic



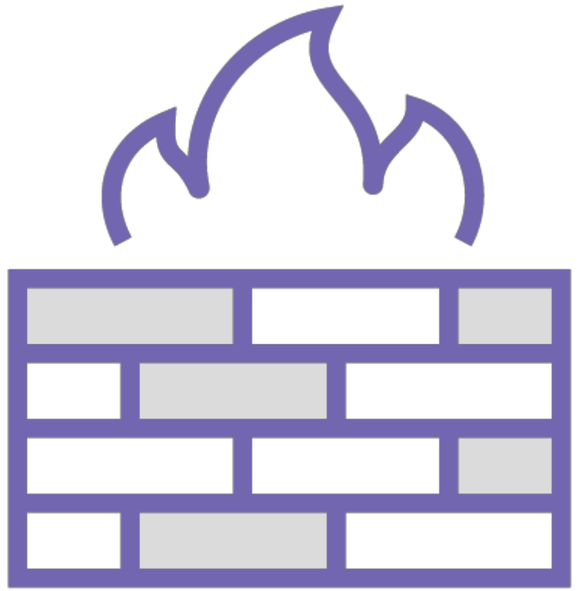
Firewall Rules

Every VPC has two permanent rules

- Implied allow egress
- Implied deny ingress

Can be overridden by more specific rules

In addition, default VPC has several rules



Additional Rules in Default VPC

default-allow-internal

default-allow-ssh

default-allow-rdp

default-allow-icmp

Auto Mode and Custom Mode VPCs

VPCs on the Google Cloud

Auto Mode

Subnets automatically created in each region, default firewall rules

Custom Mode

Manually create subnets in regions, no defaults preconfigured

Auto Mode

Subnets automatically created in each region, default firewall rules

Default VPC is an auto mode VPC

Pre-created subnets, rules

User can create additional auto mode VPCs

Custom Mode

Manually create subnets in regions, no defaults preconfigured

No subnets automatically created

Only two implied firewall rules

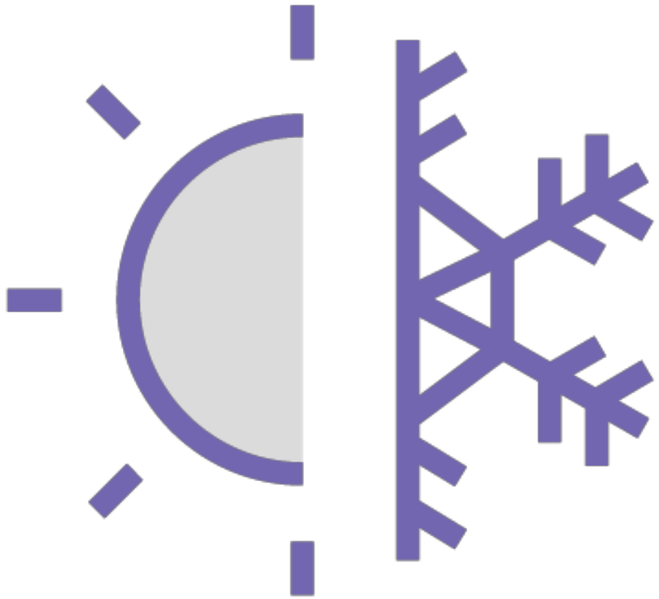
- Allow egress
- Deny ingress

Custom Mode

Manually create subnets in regions, no defaults preconfigured

Onus on user to

- Define subnets
- Associate IP ranges with each subnet
- Define firewall rules

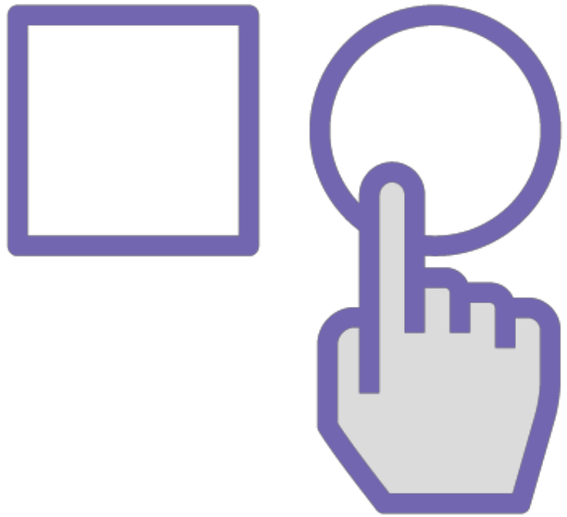


Changing VPC Mode

Auto -> Custom: Possible

Custom -> Auto: Not possible

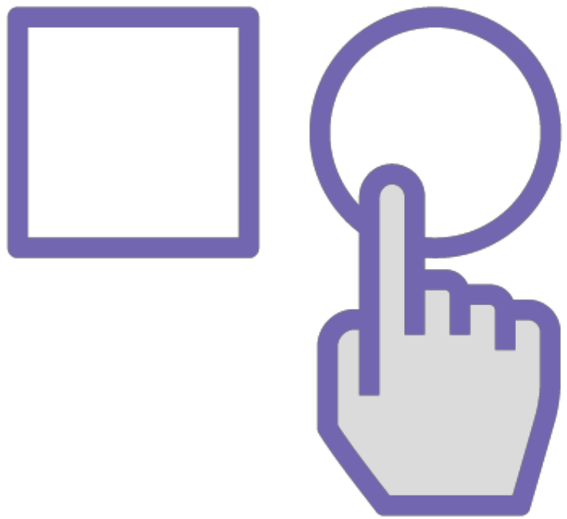
Choosing Auto Mode



Easy to use, GCP does all the work

Automatically defined ranges for all regions

Pre-defined IP ranges



Choosing Custom Mode

More control over network configuration

No need for subnets in each region

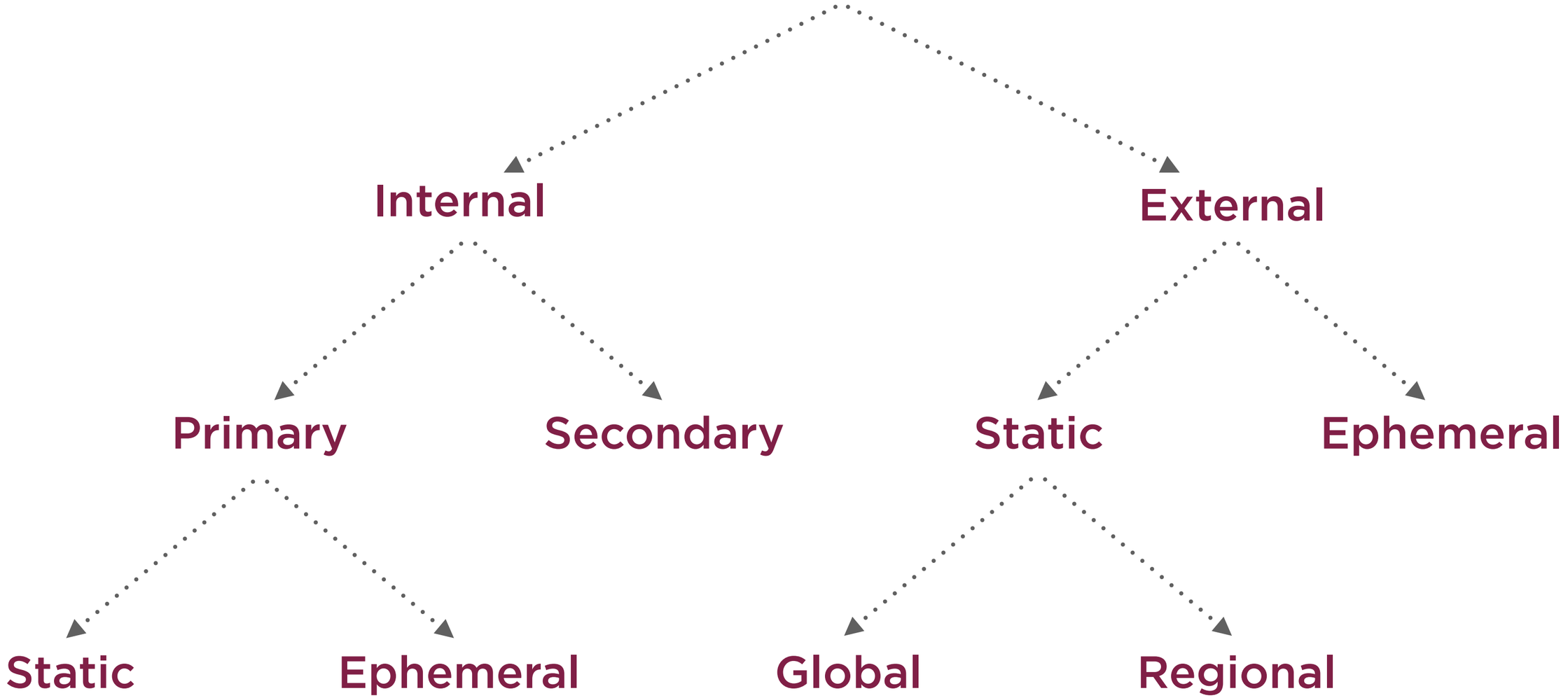
Predefined IP ranges might clash with peer network

Preferably use custom networks with

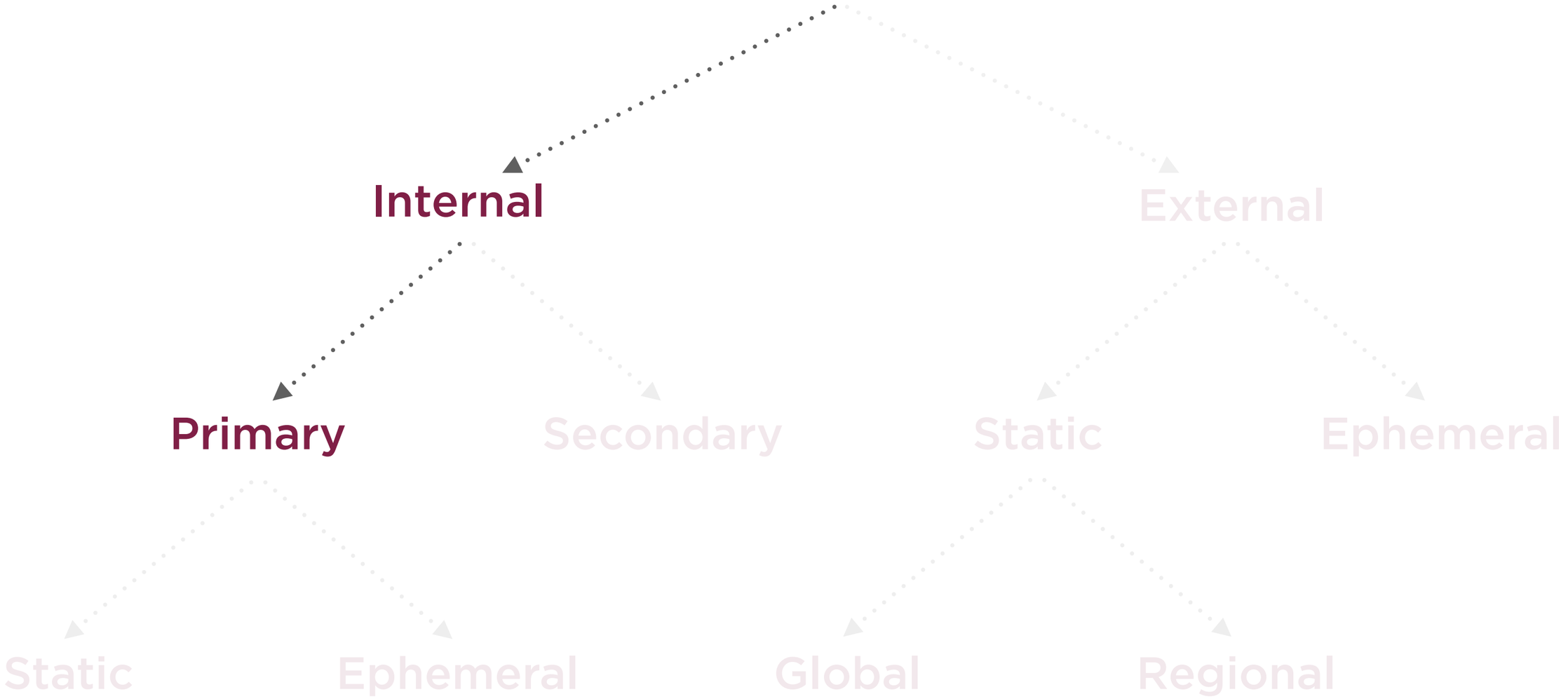
- VPC peering
- Cloud VPN

IP Addresses for GCE VM Instances

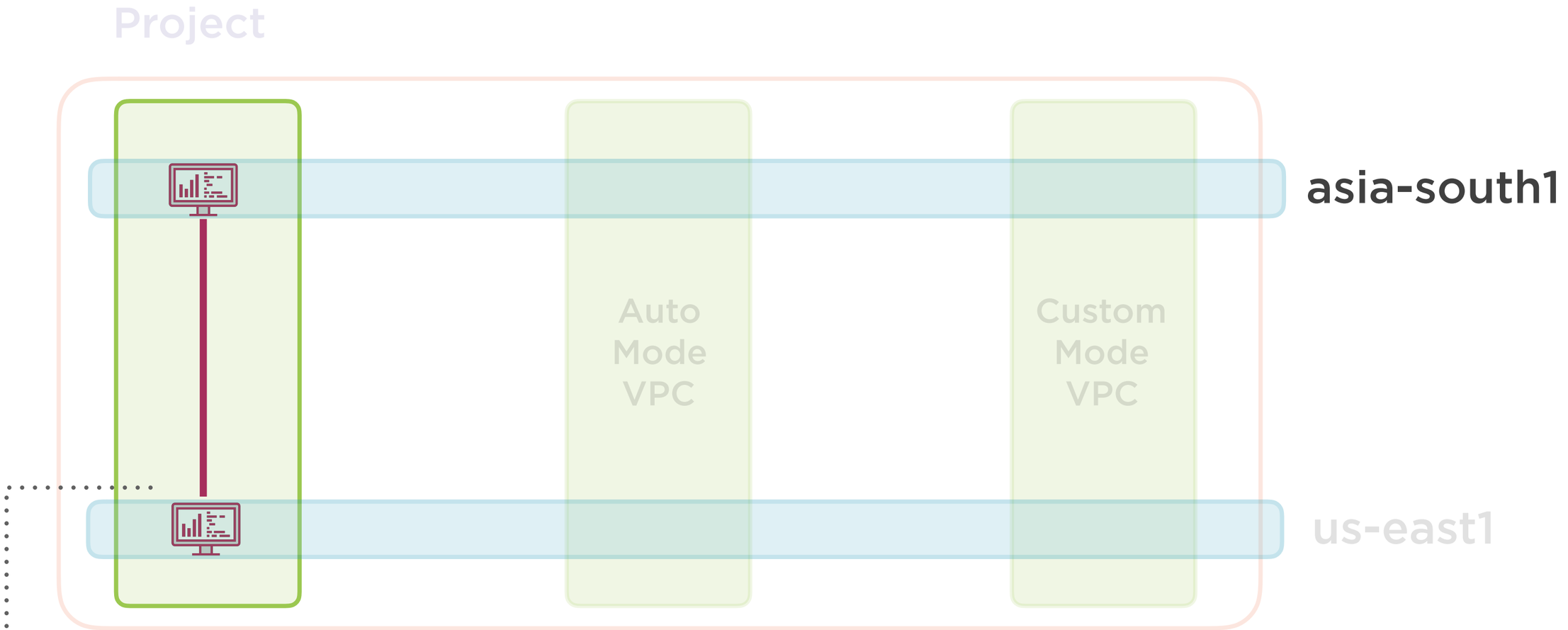
GCE VM IP Addresses



GCE VM IP Addresses

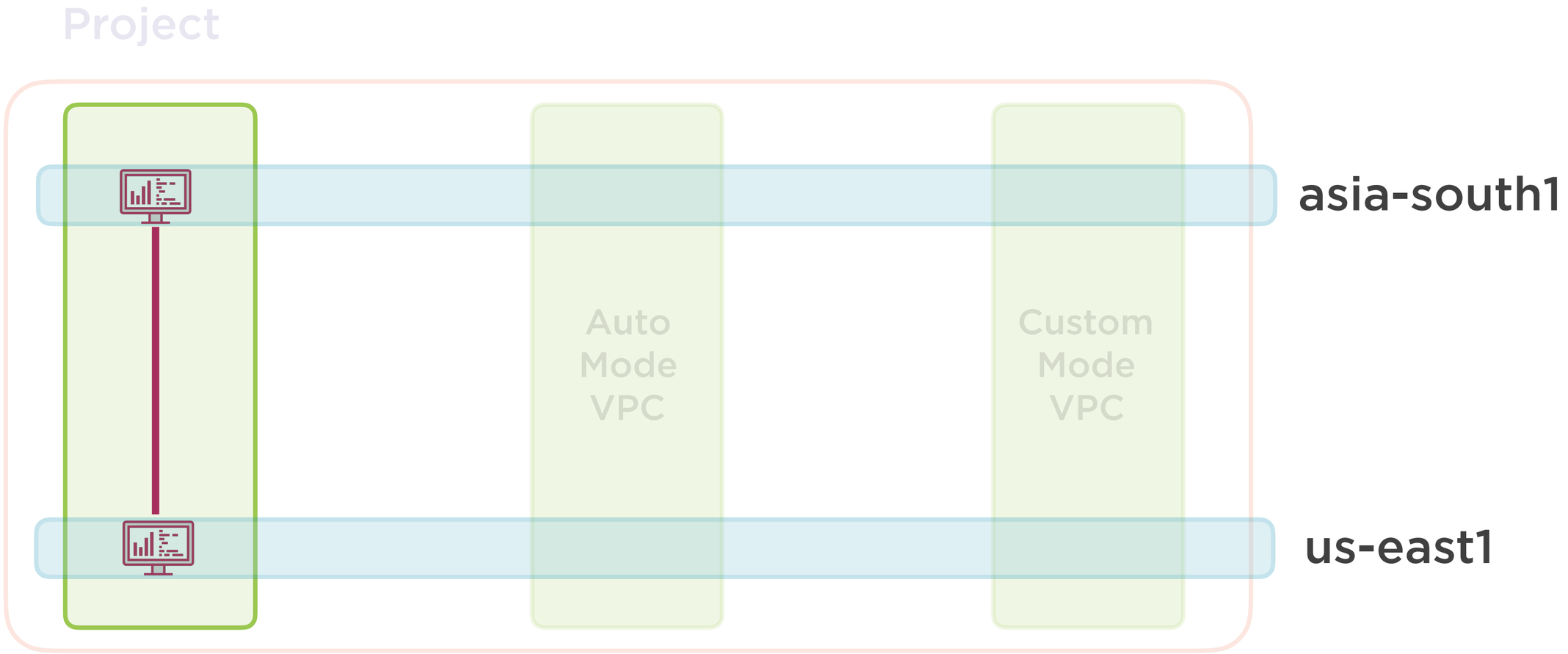


Understanding VPCs



Resources within VPC communicate using private IP addresses

Understanding VPCs



Physical location does not matter

Primary Internal IP

Every VM instance has a primary internal IP address

Unique within VPC network

Not unique across VPC networks

Primary Internal IP

Only accessible from

- Within same VPC
- From linked network
  - Shared VPC
  - VPN

Internal DNS

Project-wide DNS

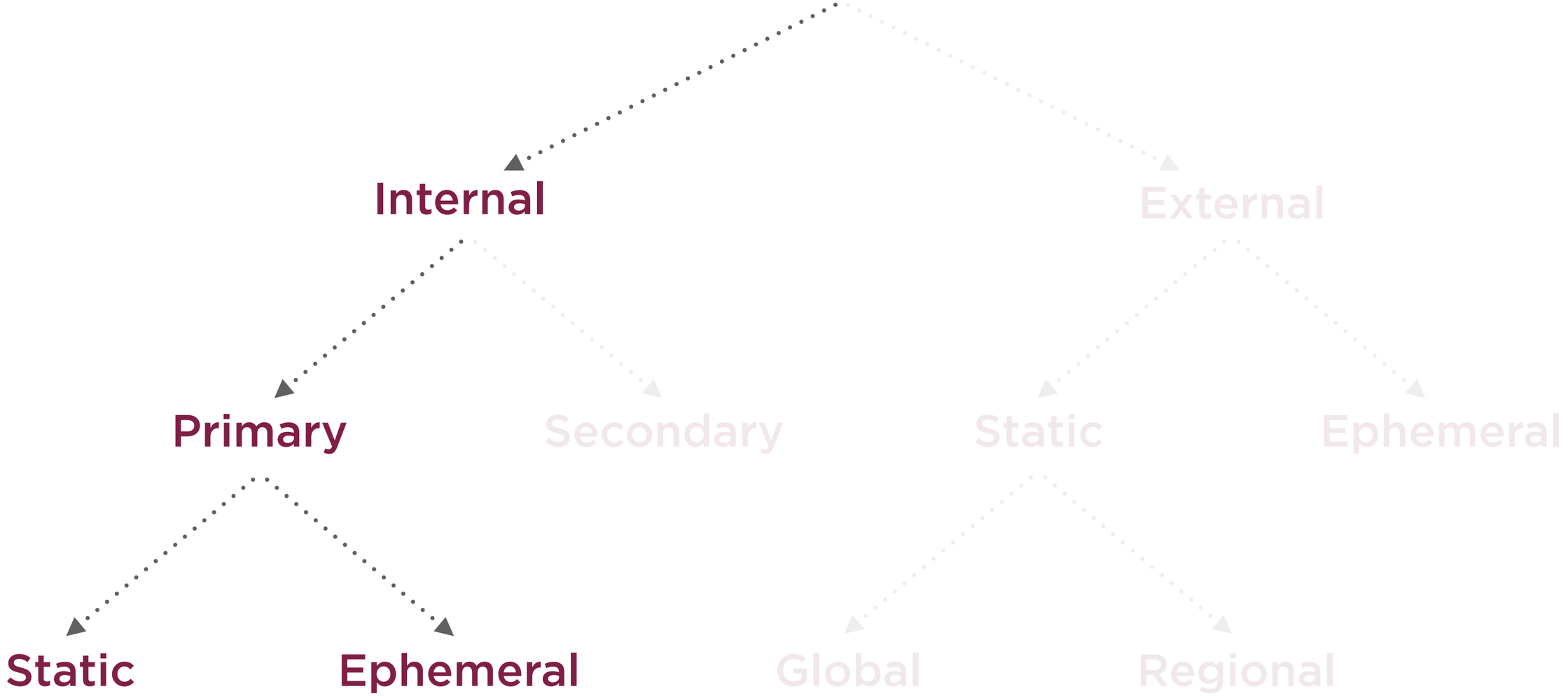
Based on instance name

Users need not rely on ephemeral IP addresses

Fully Qualified Domain Name (FQDN)

- **Zonal DNS:**
  instance_name.zone.c.project_id.internal
- **Global DNS:**
  instance_name.c.project_id.internal

GCE VM IP Addresses



Primary Internal IP

Can assign specific internal IP

Can reserve static internal IP

Else, Compute Engine assigns automatically

Must always belong to IP range of subnet

Static Internal IPs

Static internal IPs are assigned to project long-term

Held until explicitly released

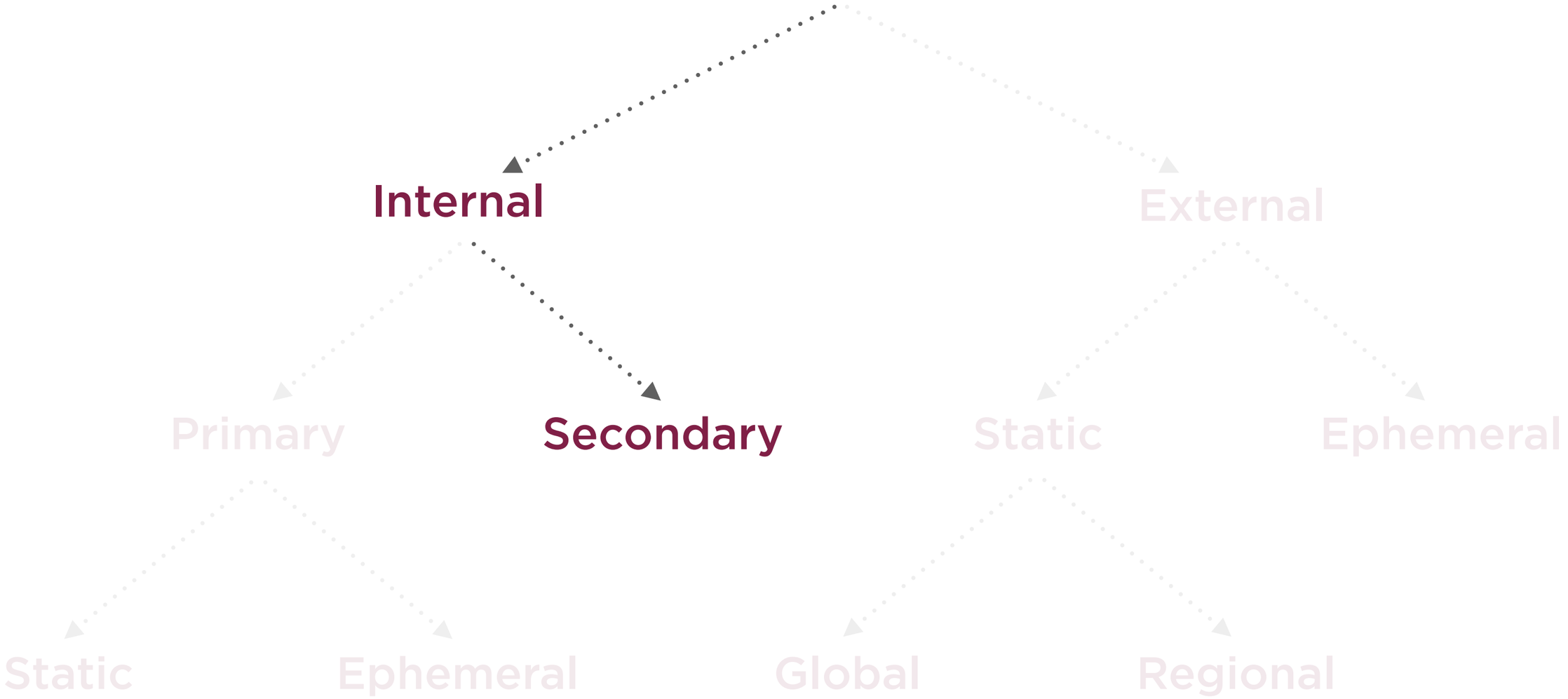
Remain attached to stopped instances

Ephemeral Internal IPs

Only attached to VM instances until VM is stopped or restarted

Upon restart, new ephemeral IP address is assigned

GCE VM IP Addresses

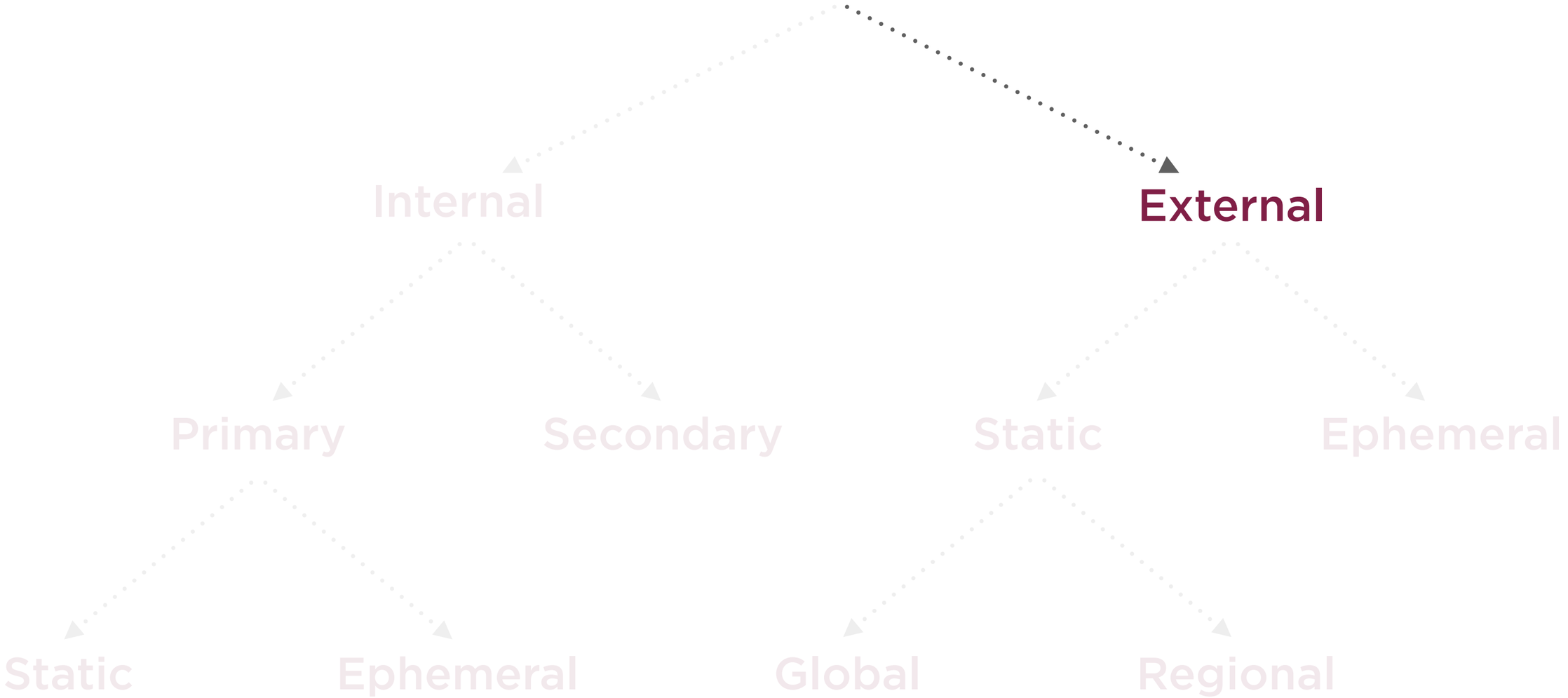


Secondary Internal IPs

If multiple services run on VM instance, can add secondary IPs

Alias IP ranges

GCE VM IP Addresses

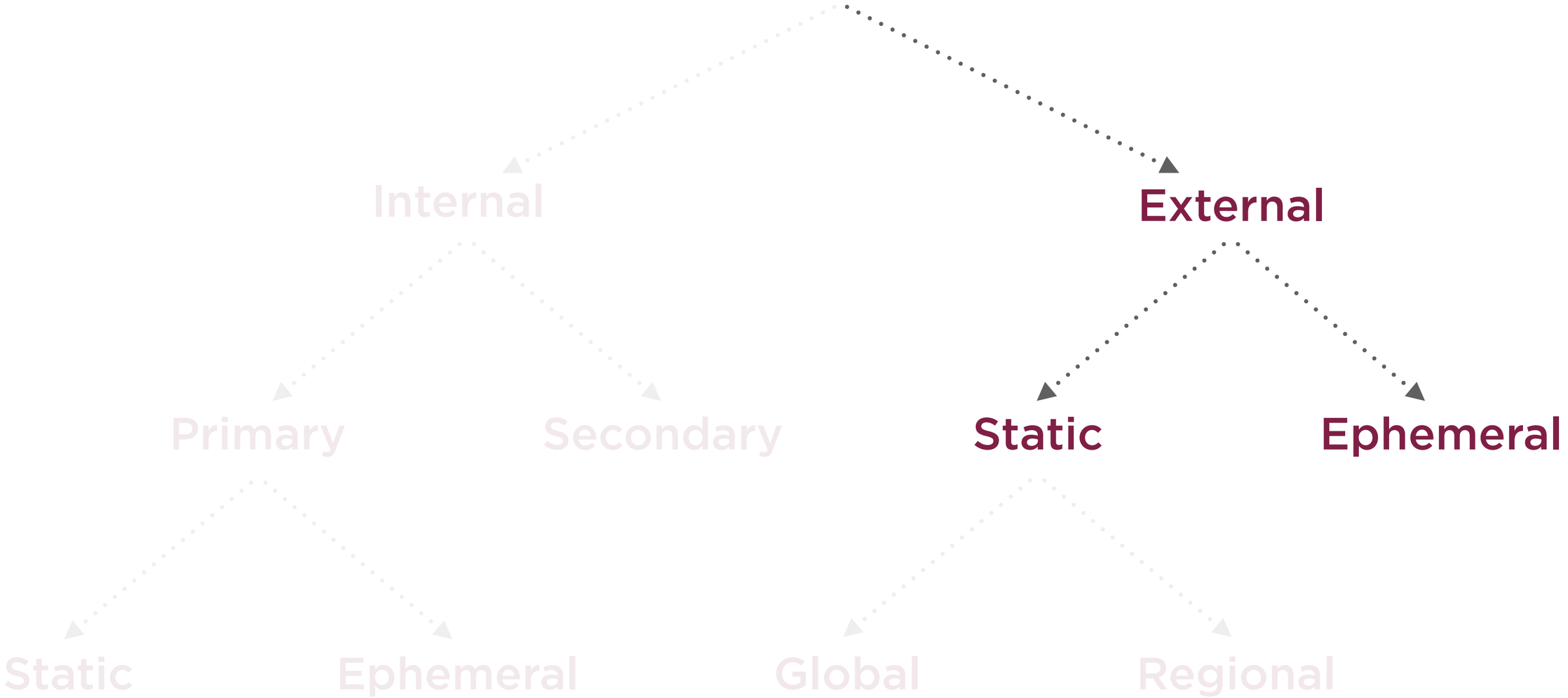


External IP Addresses

Required in order to communicate with

- Internet
- Different, unlinked VPC
- Non-GCE resources

GCE VM IP Addresses



External IP Addresses

Static: Remain attached to resource until explicitly detached

Ephemeral: Only attached until VM is stopped, restarted or terminated

External IP Addresses

Can attach external IP address to

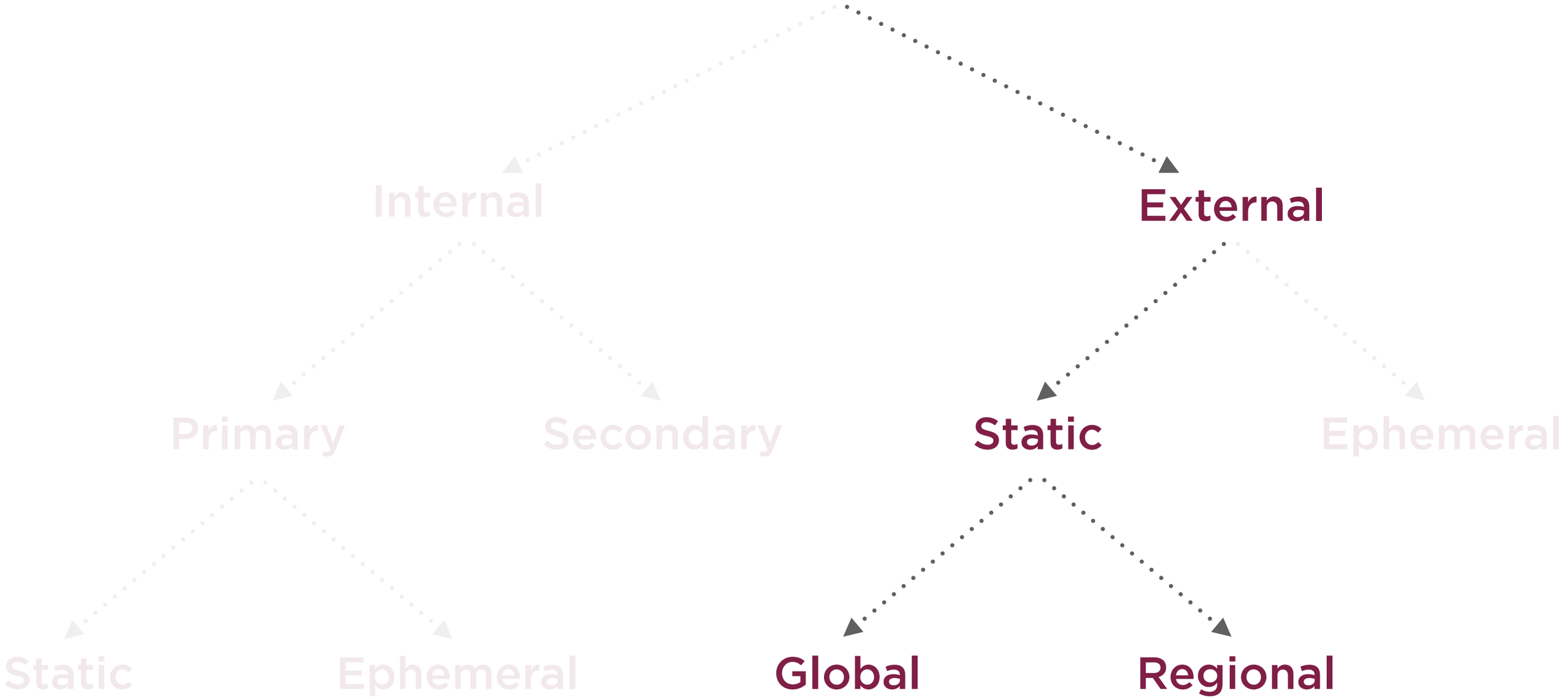
- instance
- forwarding rule (used in load balancing)

External IP Addresses

Can assign multiple external IP addresses to single instance

Need multiple forwarding rules pointing to single target instance

GCE VM IP Addresses



Demo

Studying the default auto mode network created in every project

Understanding the subnets creates, firewall rules, routes

Demo

Creating and working with auto mode VPC networks

Communicating between instances on the same network

Demo

Creating custom mode VPC networks using the web console and the gcloud command line utility

Summary

VPCs are isolated, private partitions for resources

Contain abstractions for routes, rules and IP addresses

VPCs are global, span regions

Composed of regional subnets

Auto mode and custom mode VPCs