GOOGLE CLOUD PLATFORM

VPC AND SUBNETS

WHAT IS A VPC

- A VPC network is a global resource which consists of a list of regional virtual subnetworks (subnets) in data centers
- They are all connected by a global wide area network.
- VPC networks are logically isolated from each other in GCP.
- All Compute Engine VM instances, GKE clusters, and App Engine Flex instances rely on a VPC network for communication.
- The network connects the resources to each other and to the Internet.

FEATURES

- Global
  - Single VPC across all regions
  - No cross region VPNs required
  - No peering of regional VPCs required
- Shareable
  - Single shared VCP
  - Firewalls, Routes, VPN configured once
  - Private IP space managed centrally
- Private
  - Private access to Google APIs
  - No need for public Ips to access Google services

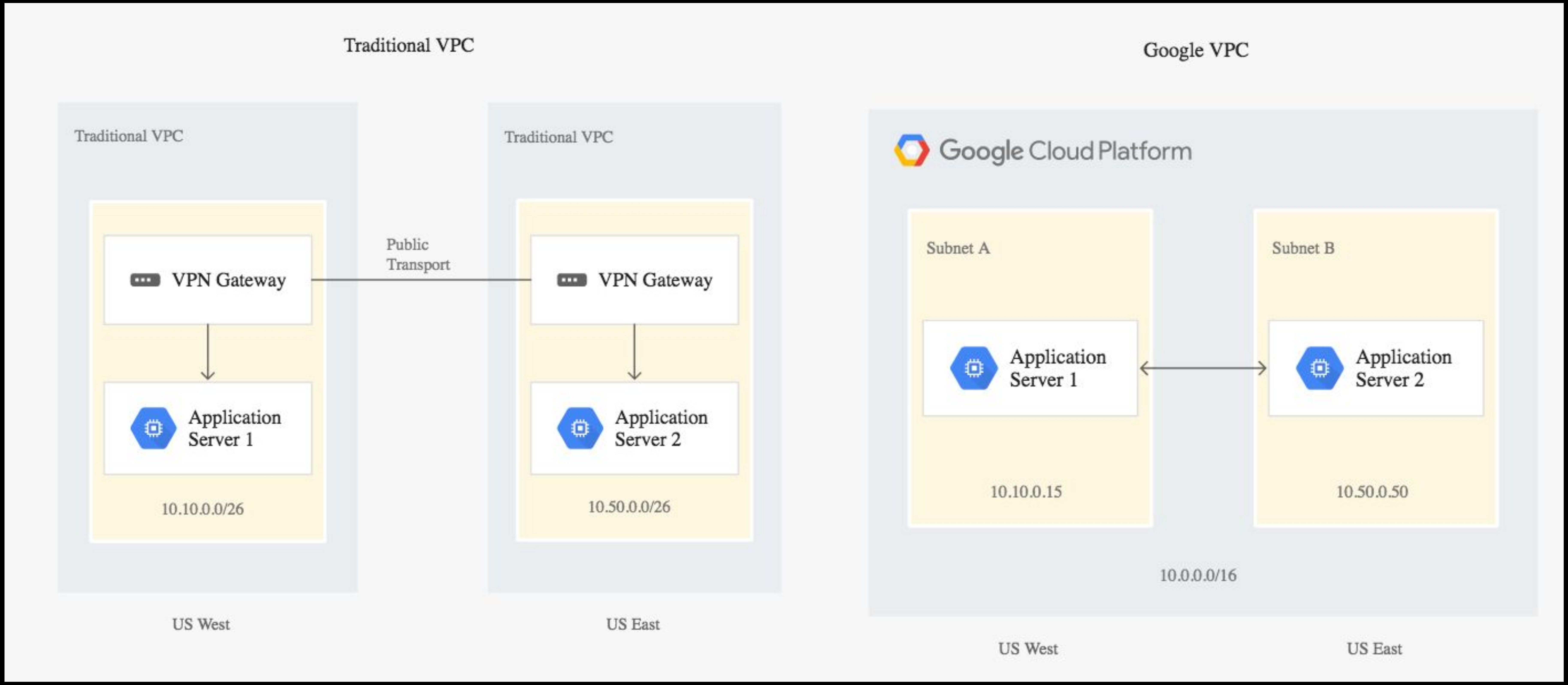
FEATURES

- Secure
  - Encryption of data in transit
  - Cloud Armor – secure the VPC perimeter
  - Distributed firewalls
- Scalable
  - Distributed network
  - No choke points
- Performance
  - High bandwidth and availability
  - Andromeda control plane
  - Support for Kubernetes via GKE

VPC CONCEPTS

- VPC networks and their associated routes/firewall rules, are global resources - *not* associated with any particular region or zone.
- A network must have at least one subnet before you can use it.
- *Subnets* are regional resources. Each subnet defines a range of IP addresses.
- When you create an instance or resource you select a zone, a network, and a subnet.
- GCP assigns the instance an IP address from the range of available addresses in the subnet.
- Traffic to and from instances can be controlled with network firewall rules.

VPC CONCEPTS



SUBNET CREATION MODE

- GCP offers two types of VPC networks – auto mode and custom mode
- When an auto mode network is created, one subnet from each region is automatically created within it’s predefined IP ranges and new subnets are added when new regions become available
- Each project starts with a default auto mode network.
- The predefined IP ranges of the subnets do not overlap with IP ranges you would use for different purposes (except for manually added ones)
- When a custom mode network is created, no subnets are automatically created.
- This type of network provides you with complete control over its subnets and IP ranges.
- You decide which subnets to create, in regions you choose, and using IP ranges you specify.

DEMO: CREATING AN AUTO MODE NETWORK

1. Go to the VPC networks page in the Google Cloud Platform Console.
2. Click Create VPC network.
3. Enter a Name for the network.
4. Choose Automatic for the Subnet creation mode.
5. In the Firewall rules section, select one or more predefined firewall rules that address common use cases for connectivity to VMs. (Or no rules).
6. Choose the Dynamic routing mode for the VPC network.
7. For more information, see dynamic routing mode. You can change the dynamic routing mode later.
8. Click Create.

SUBNETS AND IP RANGES

- When you create a subnet, you must define a primary IP address range and optionally up to five secondary IP address ranges
- **Primary IP address range**: These IP addresses can be used for VM primary internal IP addresses, VM alias IP addresses, and the IP addresses of internal load balancers.
- **Secondary IP address ranges**: These IP address ranges are used only for alias IP addresses.
- **Reserved Ips**: Every subnet has four reserved IP addresses in its primary IP range (no reserved IP addresses in the secondary IP ranges) e.g. 10.1.2.0/24
  - Network: First address in the primary IP range 10.1.2.0
  - Default Gateway: Second address in the primary IP range 10.1.2.1
  - Second-to-last Reservation: Second-to-last address range 10.1.2.254
  - Broadcast: Last address in the primary IP range 10.1.2.255

DEMO: SUBNETS

Listing and describing subnets

1. Go to the VPC networks page in the Google Cloud Platform Console.
2. Click the name of a network then click the **Subnets** tab on the **VPC network details** page to view subnets for just that network, instead of for all networks.
3. To focus on subnets for a particular network, click the name of a network. On its *VPC network details* page, click the name of a subnet in the **Subnets** tab to view its *Subnet details* page.

Adding subnets

1. Click the name of a VPC network to show its VPC network details page.
2. Click Add subnet. In the panel that appears: Provide a Name, select a Region.
3. Enter an IP address range.
4. To define a secondary range for the subnet, click Create secondary IP range.
5. Private Google access: You can enable Private Google Access for the subnet when you create it or later by editing it.
6. Flow logs: You can enable VPC flow logs for the subnet when you create it or later by editing it.
7. Click Add.

INTERFACES AND IP ADDRESSES

IP addresses

- GCP resources, such as Compute Engine VM instances, forwarding rules, GKE containers, and App Engine, rely on IP addresses to communicate.

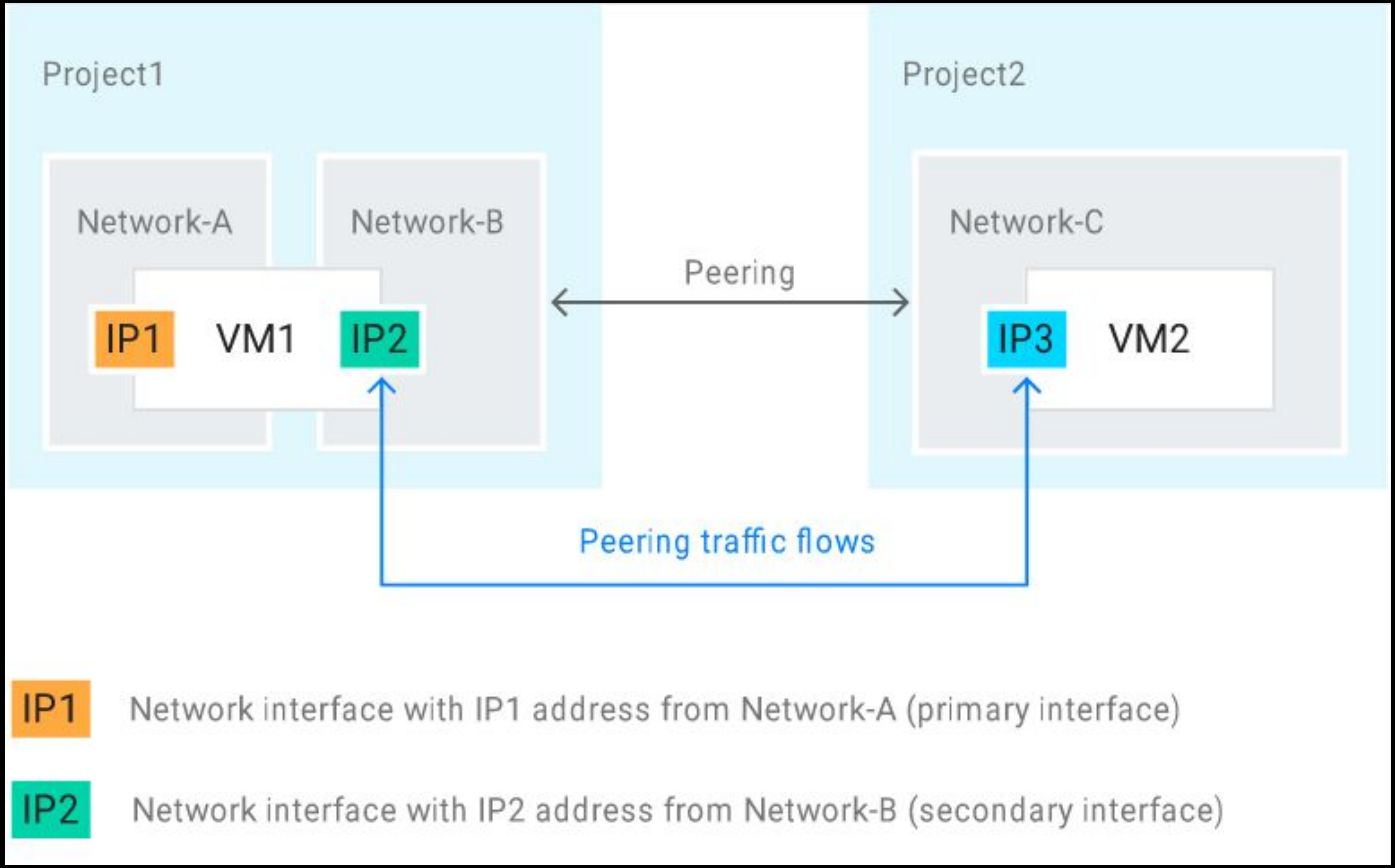
Alias IP ranges

- You can give each service a different internal IP address using Alias IP Ranges for multiple services.
- The VPC network forwards packets destined for each configured alias IP to the corresponding VM.

Multiple Network Interfaces

- You can add multiple network interfaces to a VM instance
- Each interface resides in a unique VPC network.
- Multiple network interfaces enable a network appliance VM to act as a gateway for securing traffic among different VPC networks or to and from the Internet.

MULTIPLE NETWORK INTERFACES



IP1 Network interface with IP1 address from Network-A (primary interface)

IP2 Network interface with IP2 address from Network-B (secondary interface)

ROUTES

- Routes define paths for packets leaving instances (egress traffic).
- Every new network starts with two types of system-generated routes:
  - The default route defines a path for traffic to leave the VPC network, provides general Internet access to VMs and provides the typical path for Private Google Access
  - A subnet route is created for each of the IP ranges associated with a subnet.
  - Every subnet has at least one subnet route for its primary IP range, and additional subnet routes are created for a subnet if you add secondary IP ranges to it.
  - Subnet routes define paths for traffic to reach VMs that use the subnets.
- Each VPC network has an associated *dynamic routing mode* that controls the behavior of all of its Cloud Routers.

FIREWALL RULES

- Firewall rules apply to both outgoing (egress) and incoming (ingress) traffic in the network.
- Firewall rules control traffic even if it is entirely within the network, including communication among VM instances.
- Every VPC network has two implied firewall rules – One rule allows most egress traffic, and the other denies all ingress traffic.
- For one instance to be able to communicate with another, appropriate firewall rules must also be configured because of the implied deny firewall rule for ingress traffic.
- For an instance to have outgoing Internet access, Firewall rules must allow egress traffic from the instance and it must have an external IP address.

HYBRID CLOUD & LOAD BALANCING

VPN

- Allows you to connect your VPC network to your physical, on-premises network or another cloud provider using a secure Virtual Private Network.

Interconnect

- Allows you to connect your VPC network to your on-premises network using a high speed physical connection.

Load balancing

- Global external load balancing, including HTTP(S) load balancing, SSL Proxy, and TCP Proxy offerings.
- Regional, external network load balancing
- Regional internal load balancing

VPC SHARING AND PEERING

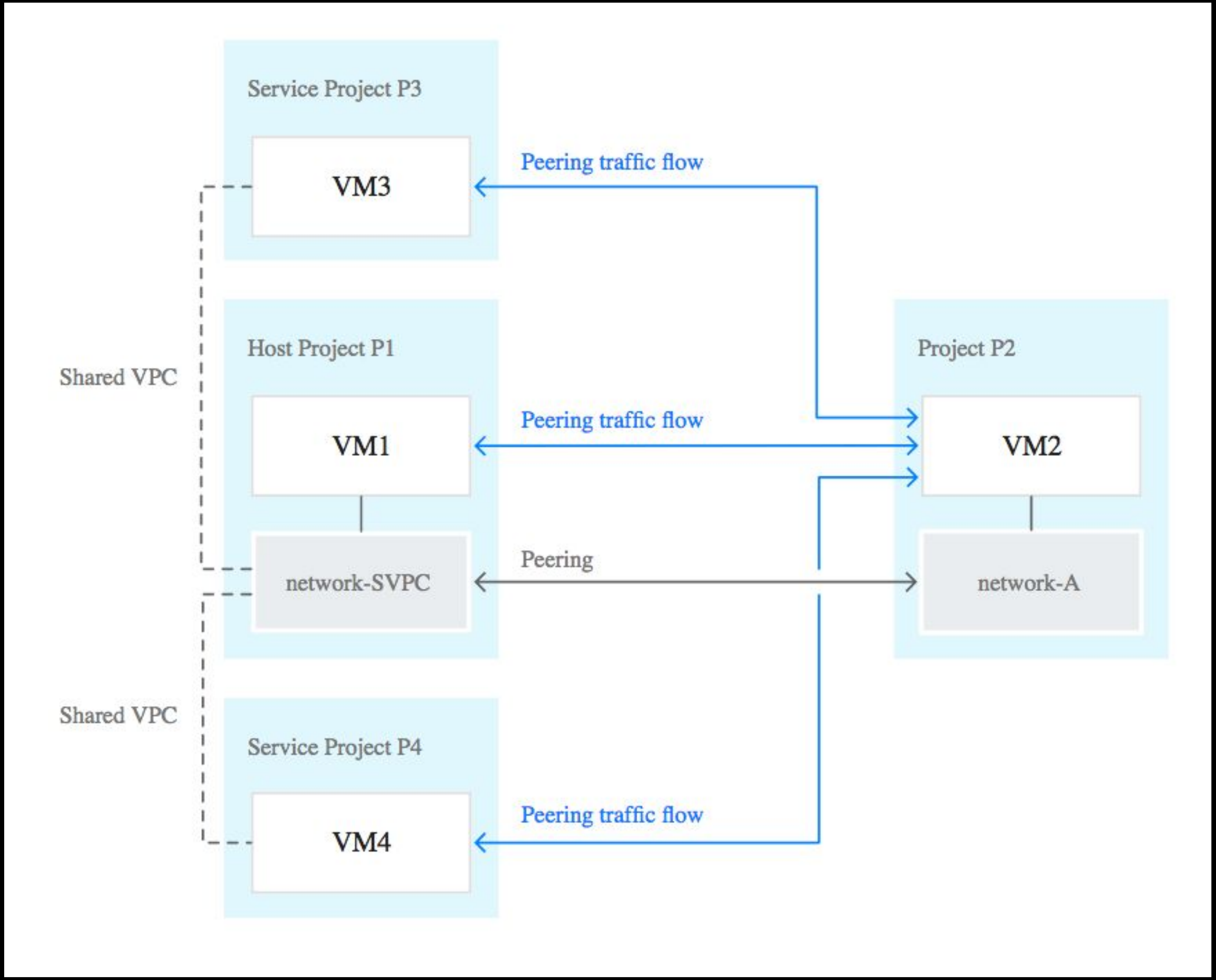
Shared VPC

- You can share a VPC network from one project (called a host project) to other projects in your GCP organization.
- You can grant access to entire Shared VPC networks or select subnets

VPC Network Peering

- Allows you to build SaaS ecosystems in GCP, making services available privately across different VPC networks
- The networks can be in the same project, different projects, or projects in different organizations.
- With VPC Network Peering, all communication happens using private, IP addresses. Subject to firewall rules

VPC SHARING AND PEERING



DEMO: CREATE SHARED VPC

Enable a host project and attach service projects

1. Go to the Shared VPC page in the Google Cloud Platform Console.
2. Select the project you want to enable as a Shared VPC host project from the project picker.
3. Click **Set up Shared VPC**.
4. On the next page, click **Save & continue** under **Enable host project**.
5. Under **Select subnets** Click **Share all subnets (project-level permissions)**
6. Click **Continue**.
   In **Project names**, specify the *service projects* to attach to the host project.
7. In the **Select users by role** section, add Service Project Admins.
8. Click **Save**.