Google Cloud VPC: Your Private Network in the Cloud

A virtual private cloud (VPC) lets you provision a logically isolated section of the Google Cloud where you can launch Google Cloud resources in a private network.

(T) **by The XYZ Company**

What is a VPC and Why Do You Need One?

Isolation

VPCs provide a logically isolated network within Google Cloud. This ensures your resources are separate from other projects.

Control

You have complete control over your network configuration. This includes IP addresses, subnets, routes, and firewalls.

Security

VPCs allow you to implement granular security policies. Use firewalls to control traffic flow and protect your resources.

VPC Architecture: Regions, Zones, and Global Reach

1

Global VPC

A VPC is a global resource. It spans multiple regions without needing extra configuration.
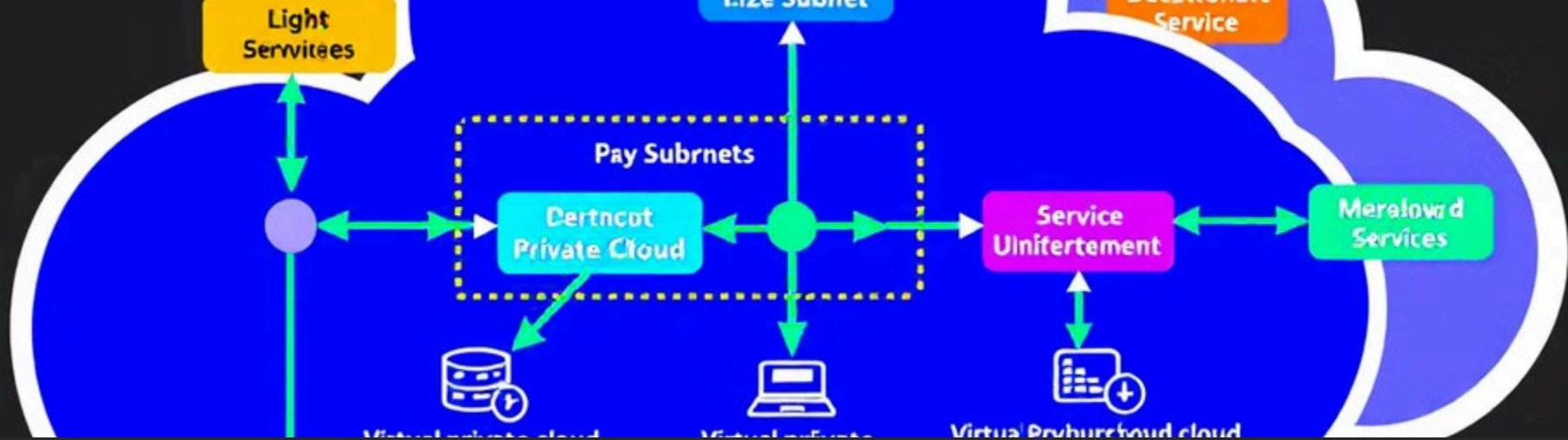
2

Regions

Regions are independent geographic areas. Deploy resources in different regions for redundancy.

3

Zones

Zones are isolated locations within a region. Distribute resources across zones for high availability.

Subnets: Dividing Your VPC for Organization and Security

1 **Subnet Definition**

Subnets are subdivisions of your VPC network. They exist within a single region.

2 **Organization**

Use subnets to organize your resources. Group resources based on function or security needs.

3 **Security Boundaries**

Subnets can act as security boundaries. Implement different firewall rules for each subnet.

IP Addressing in VPC: Internal and External

Internal IPs

Used for communication within the VPC.

External IPs

Allow resources to communicate with the internet.

Private Google Access

Enables internal IPs to access Google services.

1

2

3

Routing: Directing Traffic Within Your VPC
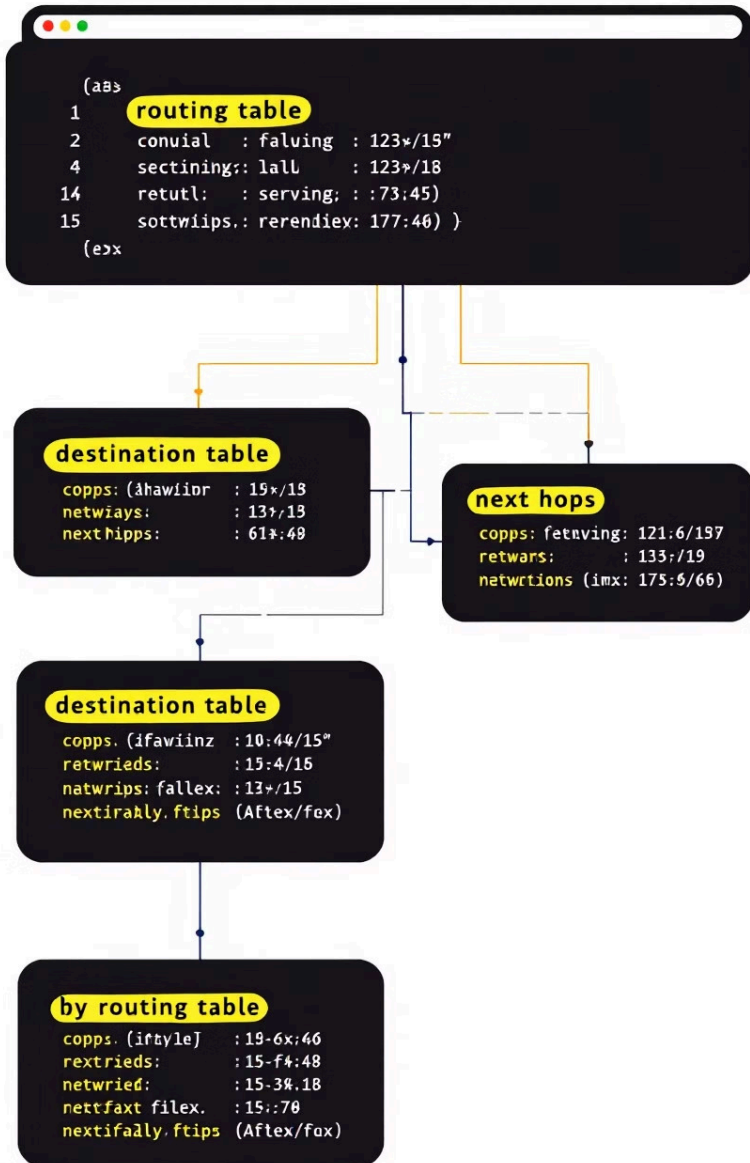
Default Routes

Automatically created routes for internal communication.

Custom Routes

Define routes to control traffic flow based on destination.

Route Priority

Determine which route is used when multiple routes apply.

Firewalls: Securing Your VPC with Rules

1 **Firewall Rules**

Control inbound and outbound traffic based on IP addresses, ports, and protocols.

2 **Implicit Rules**

Default rules that allow all outbound and block all inbound traffic.

3 **Priority**

Rules are evaluated based on priority. Lower number means higher priority.

VPC Peering: Connecting VPCs for Collaboration

Direct Connection

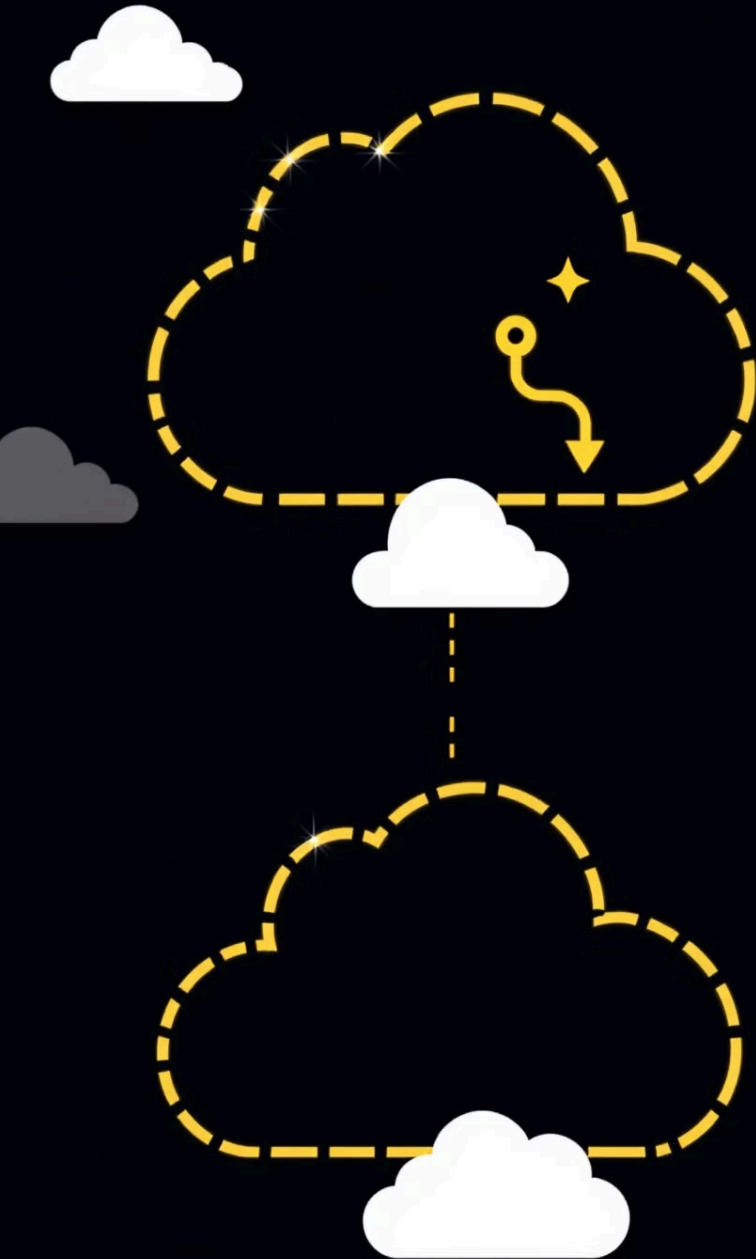Establishes a direct networking connection between two VPCs.

Private Communication

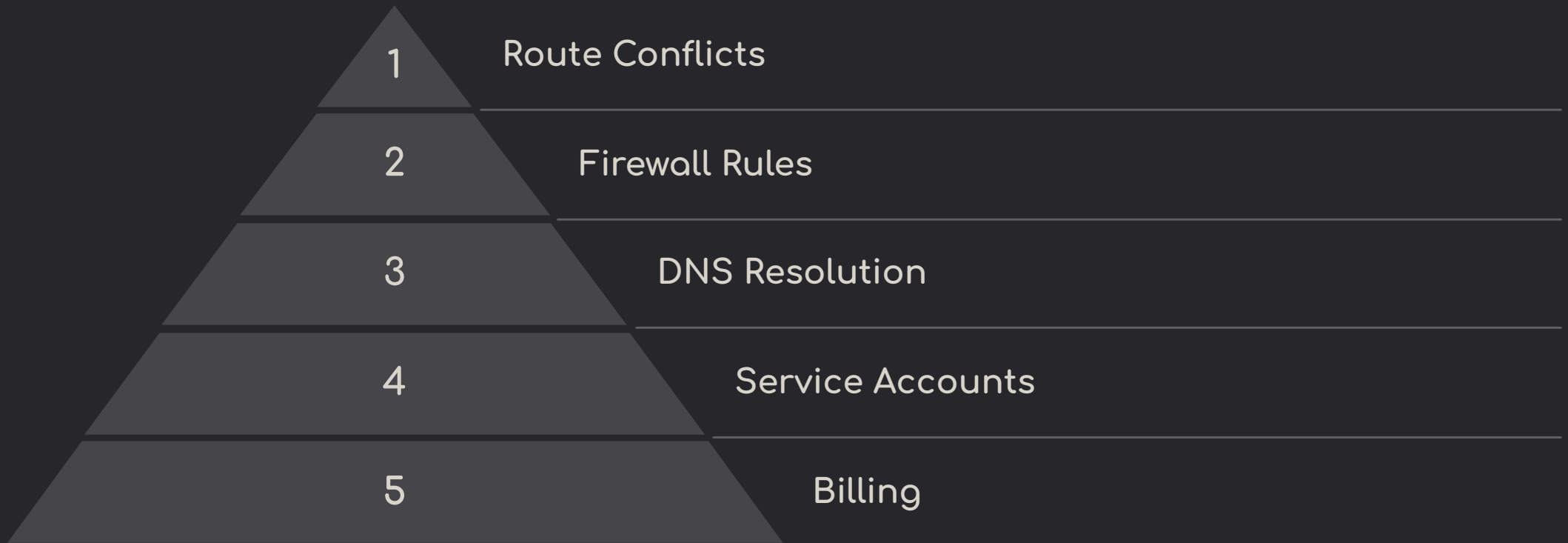Enables private IP address communication across VPCs.

Centralized Management

Allows resources in different projects to communicate without external IPs.

Points to Notice While Doing VPC Peering

1 Route Conflicts

2 Firewall Rules

3 DNS Resolution

4 Service Accounts

5 Billing

VPC Peering enables you to connect one VPC network with another one, so that resources can communicate in either network. While doing that please consider Route Conflicts, Firewall Rules, DNS Resolution, Service Accounts, and Billing.

VPC Peering Service Compatibility

Compute Services

Google Compute Engine (GCE), Google Kubernetes Engine (GKE), and App Engine flexible environment

Database Services

Cloud SQL, Cloud Memorystore, and Cloud Spanner with proper configuration

Limited Compatibility

Cloud Run, Cloud Functions, and App Engine standard environment do not support direct VPC peering connections

Note: Service compatibility may vary based on network configuration and specific deployment settings.

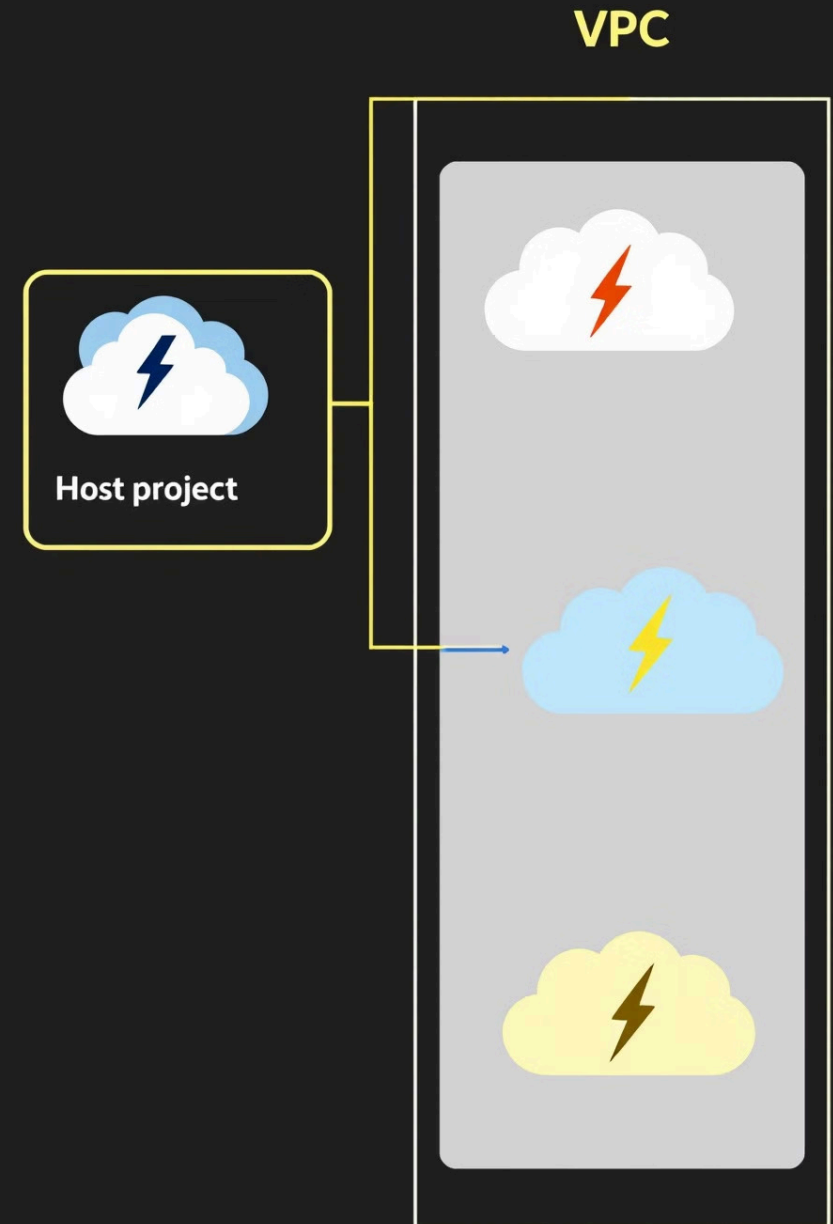# Shared VPC: Centralized Network Management

Host Project

A central project that owns the VPC network.

Service Projects

Projects that use the shared VPC network.

Centralized Control

Network administrators manage the VPC in the host project.

Cloud VPN: Securely Connecting to On-Premises Networks

IPsec VPN

Establishes an encrypted tunnel between your on-premises network and your VPC.

Secure Connection

Protects data in transit between your networks.

Hybrid Cloud

Enables you to extend your on-premises network to Google Cloud.

Cloud Interconnect: High-Bandwidth Dedicated Connections

Dedicated Interconnect	Partner Interconnect
Direct connection to Google's network.	Connect through a supported service provider.
Higher bandwidth options.	More flexible bandwidth options.