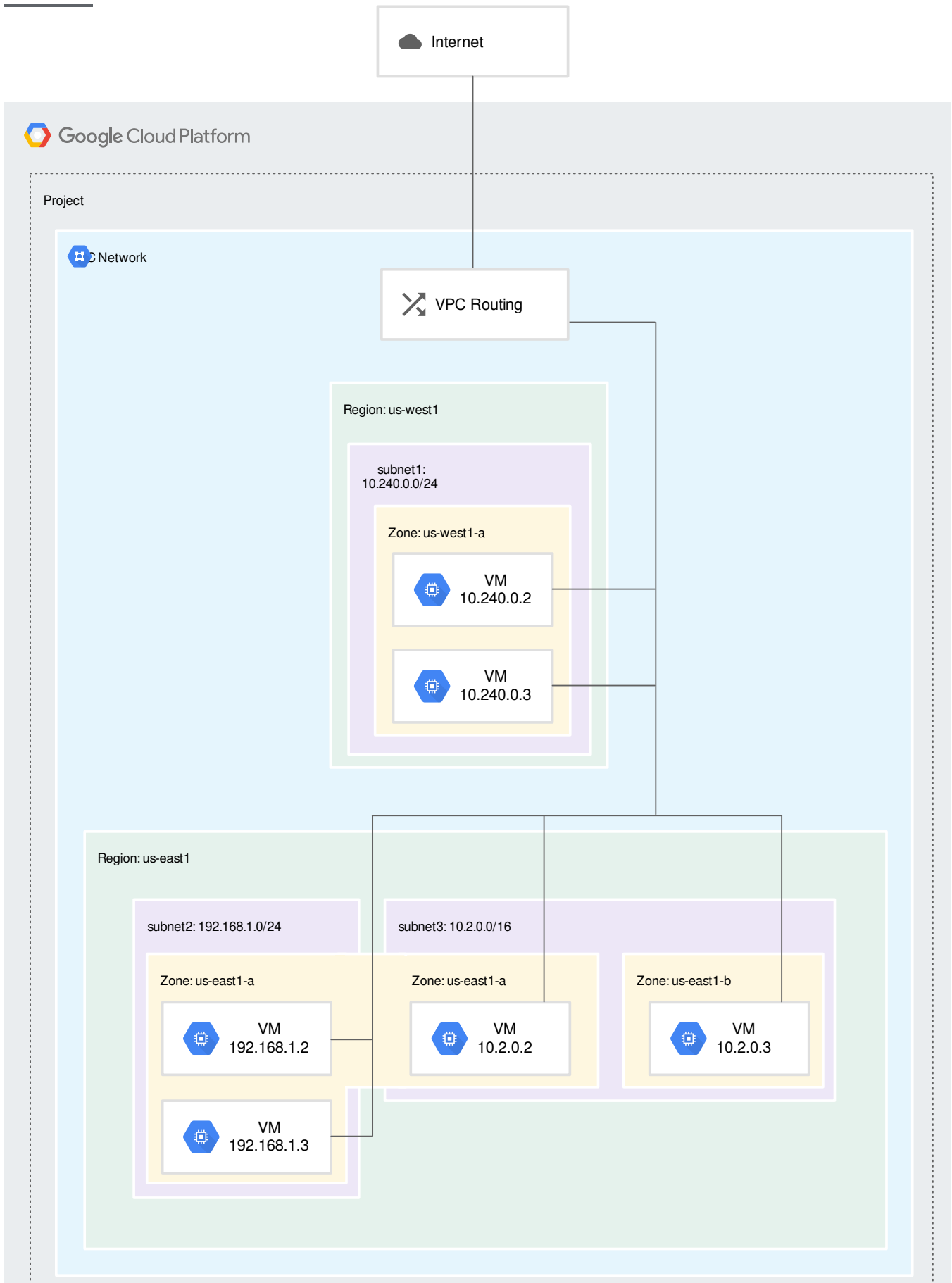



Virtual Private Cloud (VPC) provides networking functionality to [Compute Engine virtual machine \(VM\) instances](/compute/docs/instances/), [Google Kubernetes Engine \(GKE\) clusters](/kubernetes-engine/docs/), and the [App Engine flexible environment](/appengine/docs/flexible/). VPC provides networking for your cloud-based resources and services that is global, scalable, and flexible.

This page provides a high level overview of VPC concepts and features.

You can think of a VPC network the same way you'd think of a physical network, except that it is virtualized within Google Cloud. A VPC network is a global resource that consists of a list of regional virtual subnetworks (subnets) in data centers, all connected by a global wide area network. VPC networks are logically isolated from each other in Google Cloud.

VPC network example (click to enlarge)





(/vpc/images/vpc-overview-example.svg)

All Compute Engine VM instances, GKE clusters, and App Engine flexible environment instances rely on a VPC network for communication. The network connects the resources to each other and to the internet.

Read more about [VPC networks](/vpc/docs/vpc) (/vpc/docs/vpc).

Each VPC network implements a distributed virtual firewall that you can configure. Firewall rules allow you to control which packets are allowed to travel to which destinations. Every VPC network has two [implied firewall rules](/vpc/docs/firewalls#default_firewall_rules) (/vpc/docs/firewalls#default_firewall_rules) that block all incoming connections and allow all outgoing connections.

The **default** network has [additional firewall rules](/vpc/docs/firewalls#more_rules_default_vpc) (/vpc/docs/firewalls#more_rules_default_vpc), including the **default-allow-internal** rule, which permit communication among instances in the network.

Read more about [firewall rules](/vpc/docs/firewalls) (/vpc/docs/firewalls).

Routes tell VM instances and the VPC network how to send traffic from an instance to a destination, either inside the network or outside of Google Cloud. Each VPC network comes with some [system generated routes](/vpc/docs/vpc#system-generated-routes) (/vpc/docs/vpc#system-generated-routes) to route traffic among its subnets and send traffic from [eligible instances](/vpc/docs/vpc#internet_access_reqs) (/vpc/docs/vpc#internet_access_reqs) to the internet.

You can create custom static routes to direct some packets to specific destinations. For example, you can create a route that sends all outbound traffic to an instance configured as a [NAT gateway](/vpc/docs/special-configurations#natgateway) (/vpc/docs/special-configurations#natgateway).

Read more about [routes](/vpc/docs/routes) (/vpc/docs/routes).

While routes govern traffic leaving an instance, forwarding rules direct traffic to a Google Cloud resource in a VPC network based on IP address, protocol, and port.

Some forwarding rules direct traffic from outside of Google Cloud to a destination in the network; others direct traffic from inside the network. Destinations for forwarding rules are target instances, load balancer targets (target proxies, target pools, and backend services), and Cloud VPN gateways.

Read more about [forwarding rules](/compute/docs/protocol-forwarding) (/compute/docs/protocol-forwarding).

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

Read more about [IP addresses](/compute/docs/ip-addresses/) (/compute/docs/ip-addresses/).

If you have multiple services running on a single VM instance, you can give each service a different internal IP address by using alias IP ranges. The VPC network forwards packets that are destined to a particular service to the corresponding VM.

Read more about [alias IP ranges](/vpc/docs/alias-ip) (/vpc/docs/alias-ip).

You can add multiple network interfaces to a VM instance, where 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.

Read more about [multiple network interfaces](/vpc/docs/multiple-interfaces-concepts) (/vpc/docs/multiple-interfaces-concepts).

You can share a VPC network from one project (called a host project) to other projects in your Google Cloud organization. You can grant access to entire Shared VPC networks or select subnets therein by using [specific IAM permissions](/vpc/docs/shared-vpc#iam_in_shared_vpc). This allows you to provide centralized control over a common network while maintaining organizational flexibility. Shared VPC is especially useful in large organizations.

Read more about [Shared VPC](/vpc/docs/shared-vpc).

VPC Network Peering allows you to build ([software as a service \(SaaS\)](https://wikipedia.org/wiki/Software_as_a_service)) ecosystems in Google Cloud, making services available privately across different VPC networks, whether the networks are in the same project, different projects, or projects in different organizations.

With VPC Network Peering, all communication happens by using private [RFC 1918](https://tools.ietf.org/html/rfc1918) IP addresses. Subject to firewall rules, VM instances in each peered network can communicate with one another without using external IP addresses.

Peered networks share subnet routes. Optionally, both networks can be configured to share custom static and dynamic routes too. Network administration for each peered network is unchanged: Network Admins and Security Admins for one network do not automatically get those roles for the other network in the peering relationship. If two networks from different projects are peered, project owners, editors, and Compute Instance Admins in one project do not automatically receive those roles in the project that contains the other network.

Read more about [VPC Network Peering](/vpc/docs/vpc-peering).

Cloud VPN allows you to connect your VPC network to your physical, on-premises network or another cloud provider by using a secure [virtual private network](https://wikipedia.org/wiki/Virtual_private_network).

Read more about [Cloud VPN \(/vpn/docs/\)](/vpn/docs/).

Cloud Interconnect allows you to connect your VPC network to your on-premises network by using a high speed physical connection.

Read more about [Cloud Interconnect \(/interconnect/docs/\)](/interconnect/docs/).

Google Cloud offers the following load balancing configurations to distribute traffic and workloads across many VMs:

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

Read more about [Cloud Load Balancing \(/load-balancing/docs/\)](/load-balancing/docs/).

When you enable Private Google Access for a subnet, instances in a subnet of a VPC network can communicate with [Google APIs and services \(https://developers.google.com/apis-explorer/\)](https://developers.google.com/apis-explorer/) by using private IP addresses instead of external IP addresses.

Read more about [Private Google Access \(/vpc/docs/private-access-options/\)](/vpc/docs/private-access-options/).

