Google Cloud

Guide to Virtual Private Cloud (VPC)

You've learned about how virtual private clouds (VPCs) are a key component of a cloud environment. VPCs allow organizations to isolate, secure, control their resources through segmentation, firewalls, and virtual private networks (VPNs). VPCs form the foundation of network security in a cloud environment which makes it an integral concept for cloud security. In this reading, you'll learn about creating a VPC using gcloud and the Google Cloud console. You'll also learn about configuring subnets and gcloud commands related to network configuration.

Virtual Private Cloud (VPC)

In Google Cloud, a **virtual private cloud** (**VPC**) is a private cloud hosted within a public cloud, enabling organizations to use the public cloud's resources while being completely isolated from other cloud users.
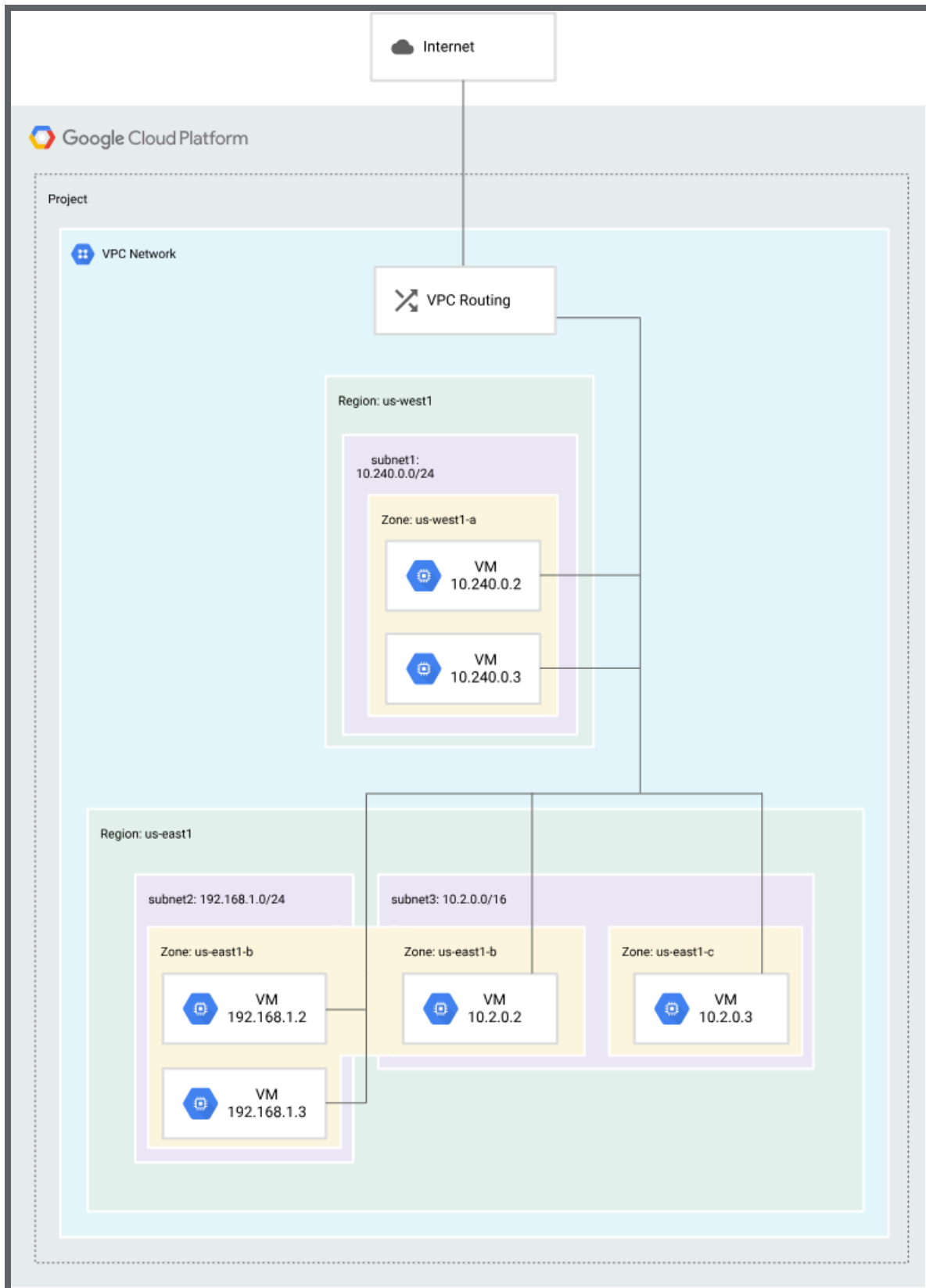
VPCs provide networking functionality to cloud-based resources and services such as Compute Engine virtual machine (VM) instances. VPC networks are logically isolated from each other in Google Cloud. A VPC network and its components such as its routes and firewall rules are *global* resources. This means that they are not associated with a region or zone and can be accessed by any resource in any zone within the same project. A VPC consists of a list of regional virtual subnetworks–also known as subnets–in data centers, all connected by a global wide area network (WAN).

Subnets in a VPC network

In computer networking, subnetting divides a network into logical groups known as subnets. Subnetting splits a large group of internet protocol (IP) addresses into smaller portions, which has many benefits including improving network efficiency and management. Each subnet specifies a range of IPv4 addresses which can be split into smaller and more manageable portions.

In Google Cloud, subnets are configured in a VPC network. Subnets are *regional* resources. This means that they are only accessible by resources within the same region.

The following diagram illustrates a VPC network with two regions: **us-west1** and **us-east1**. Each region has their own respective subnets, zones, and resources.

Google Cloud

Auto and custom mode VPC networks

There are two types of VPC networks you can choose to create depending on your subnet requirements, *auto* mode or *custom* mode.

- **Auto mode**: An auto mode VPC automatically creates a subnet in each region using predefined IPv4 ranges.
- **Custom mode**: A custom mode VPC does not automatically create subnets. Instead, you manually create and add subnets using IPv4 and IPv6 addresses.

Each new VPC that you create must have a unique name within the same project. You can create up to four additional VPC networks in a project.

Create a VPC using Cloud Shell

The Cloud Shell provides command-line access to computing resources hosted on Google Cloud. The gcloud command-line tool is pre-installed in Cloud Shell which allows you to quickly start creating and managing your cloud resources.

You can use the Google Cloud Cloud Shell to create and manage Google Cloud resources with the gcloud compute networks command to list, create, and delete Compute Engine networks.

Note: In the lab, a student user account will be automatically configured; the information about this account including the email and password can be found in the **Lab Details** panel. Use these temporary credentials to access the console.

Here is a breakdown of the syntax for gcloud compute networks which is used to configure VPC networks:

```
Unset
gcloud compute networks GROUP | COMMAND FLAGS
```

- GROUP specifies which set of subcommands you want to use. An example of a group is subnets which enables you to list, describe, delete, and update Compute Engine subnetworks.
- COMMAND specifies the action you want to perform. For example, you can use the command create to create a network or delete to delete a network.
- FLAGS in gcloud enable you to customize gcloud commands. They are double hyphens. They are prepended with double hyphens (--). Global flags apply to all gcloud commands while command-specific flags apply to certain commands. For example,

--subnet-mode=custom is a flag specific to the create command that you can use to specify the subnet mode of a VPC network.

Now that you're familiar with the basic syntax, you can explore the following commands you can use to create and configure networks on Cloud Shell:

Create a new custom mode network with the name example-vpc

```
Unset
gcloud compute networks create example-vpc --subnet-mode=custom
```

List all networks in the current project

```
Unset
gcloud compute networks list
```

Create a subnet with the name example-vpc-sub for the VPC example-vpc in the region us-west1 with an IPv4 range of 10.0.0.0/28

```
Unset
gcloud compute networks subnets create example-vpc-sub
   --network example-vpc
   --region us-west1
   --range 10.0.0.0/28
```

List all the subnets for the network named example-vpc

```
Unset
gcloud compute networks subnets list --network=example-vpc
```

Create a VPC using Google Cloud console

You can also create a VPC using the Google Cloud console.

1. In the Google Cloud console, click the **Navigation** menu (≡).
2. Click **VPC network** > **VPC networks**, and then click **+ Create VPC Network**.
3. Specify the subnets, firewall rules, and any other additional configurations.
4. Click **Create**.

Pro tip: The **Equivalent command line** link is a feature located at the bottom of the **Create a VPC Network** page. It generates the Cloud Shell commands with the parameters you selected for the VPC network so that you can easily create the resource in the Cloud Shell.

Key takeaways

Networks are the foundation of any IT infrastructure and in the cloud, creating and configuring VPC networks is as simple as clicking a couple of buttons and constructing commands on the command-line. It's important to know that VPCs must be carefully configured to meet an organization's security requirements using security controls like firewall rules, segmentation, and more.

Resources for more information

- For more information about gcloud compute network commands, check out the gcloud compute networks reference document.