Google Cloud Computing Foundation Course
Priyanka Vergardia
Google Cloud

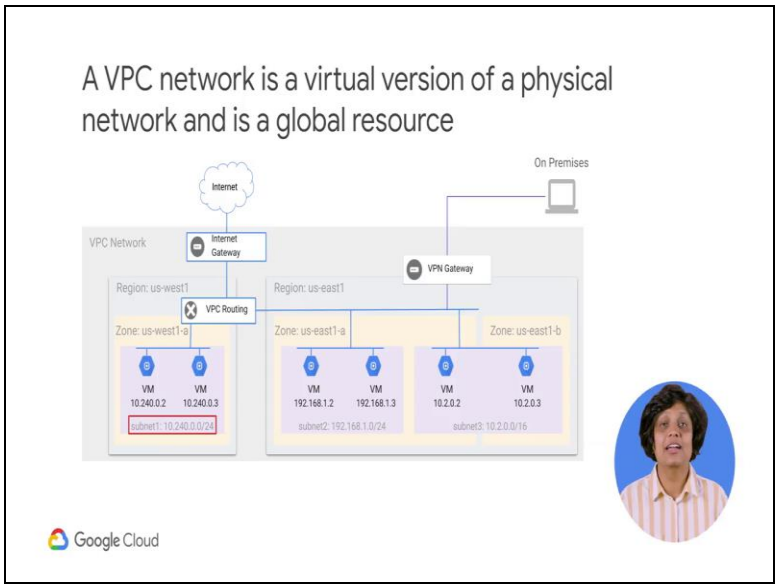
Lecture-53
Defining a Virtual Private Cloud

(Refer Slide Time: 00:05)

In this topic you will explore what a virtual private cloud is. Virtual private cloud networks or VPC's are used to build private networks on top of the larger Google network. With VPC's you can apply many of the same security and access control rules as if you were building a physical network. VPC's allow the deployment of infrastructure-as-a-service resources such as compute instances and containers.

They have no IP address ranges or global and span all available GCP regions. VPC's also contains sub networks that span all zones in a region and can have default auto or custom modes. Sub networks are also referred to as subnets. Subnets are regional resources they must be created in VPC networks to define sets of usable IP ranges for instances. VMs in different zones within the same region can share the same subnet.

(Refer Slide Time: 01:00)

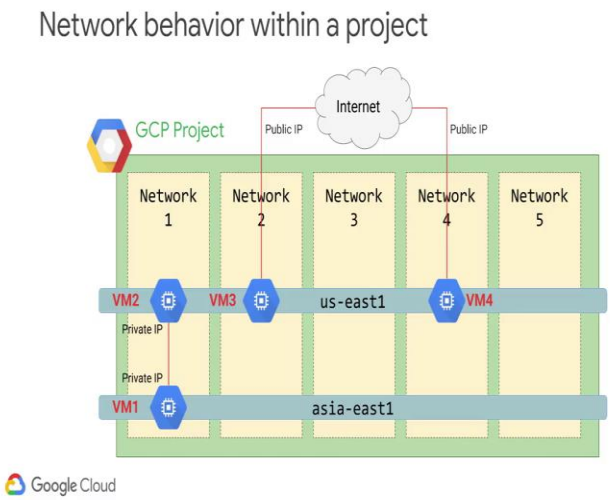


In this example subnet 1 is defined as 10 dot 240 dot 0 dot 0 / 24 in the US west region 2 VM instances in the US west 1 a zone are in this subnet. Their IP addresses both come from the available range of addresses in subnet 1. Subnet 2 is defined as 192 dot 168 dot 1 dot 0 / 24 in the US east one region 2 VM instances in the US east one a zone are in this subnet their IP addresses both come from the available range of addresses in subnet 2.

Subnet 3 is defined as 10 dot 2 dot 0 dot 0 / 16 also in the US east one region 1 VM instance in the US east one a zone and a second instance in the US east 1 b zone are in subnet 3 each receiving an IP address from its available range. Because subnets are regional resources instances can have their network interfaces associated with any subnet in the same that contains their zones. A single VPN can be used to give private connectivity from a physical data center to the VPC.

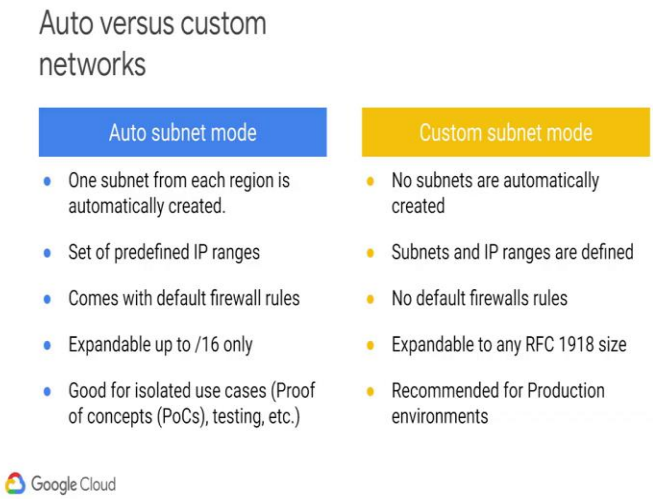
Subnets are defined by an internal IP address prefix range and are specified as cider notations. Cider stands for classless inter-domain routing. IP ranges cannot overlap between subnets they can be expanded but can never shrink. While IP ranges are specific to one region they can cross zones within the region. You can also create multiple subnets in a single region although subnets do not need to conform to a hierarchical IP scheme the internal IP ranges for a subnet must conform to RFC 1918.

(Refer Slide Time: 03:04)



Virtual machines that are in different regions but in same VPC can communicate privately. VM 1 and VM 2 can communicate at a local level even though they are separated geographically. Virtual machines that reside in different we VPC's even if the subnets are in the same region need to communicate via the internet. In this instance VM3 and VM4 will need public IP addresses to traverse the internet networks do not communicate with any other network by default.

(Refer Slide Time: 03:41)



GCP offers two types of VPC networks determined by their subnet creation mode. When an auto mode network is created one subnet from each region is automatically created within it. As new GCP regions become available new subnets and those regions are automatically added to the

auto mode networks the automatically created subnets use a set of predefined IP ranges and default firewall rules are applied.

In addition to the automatically created subnets you can add more subnets manually to auto mode networks in regions you choose using IP ranges outside set of predefined IP ranges. When expanding the IP range in an auto mode Network the broadest prefix you can use is slash 16any prefix broader than slash 16 would conflict with the primary IP ranges of other automatically created subnets. Due to its limited flexibility an auto mode network is better suited to isolated use cases such as proof of concept testing and so on.

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 subnet to create in regions you choose and using IP ranges you specify. You also define the firewall rules and you can expand the IP ranges to any RFC 1918 size. Custom mode networks are therefore a lot more flexible and are better suited to production environments.

While you can switch a network from auto mode to custom mode this conversion is one way. Custom mode networks cannot be changed to auto mode networks.