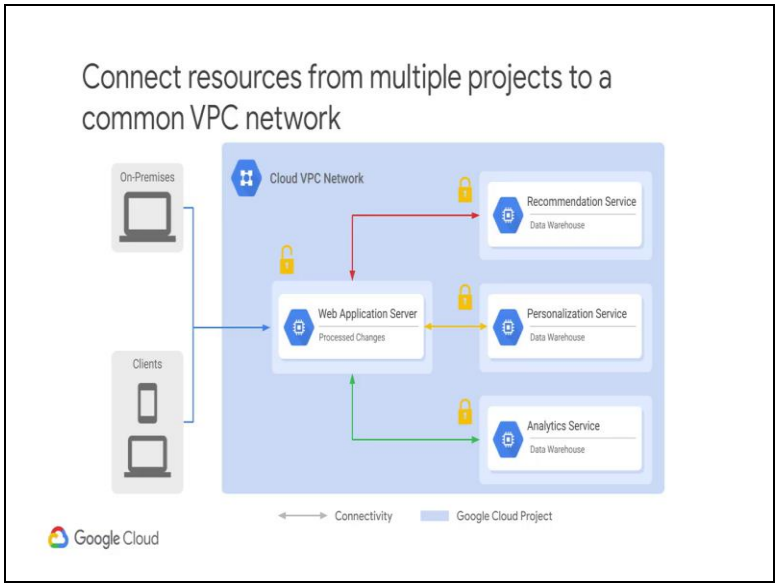
Google Cloud Computing Foundation Course
Priyanka Vergardia
Google Cloud

Lecture-57
Multiple VPC Networks

In this next topic, you will find out how to utilize multiple VPC is used to build robots networking solutions. Shared VPC allows an organization to connect resources from multiple projects to a common VPC network. This allows the resources to communicate with each other securely and efficiently using internal IP from that Network.

(Refer Slide Time: 00:22)



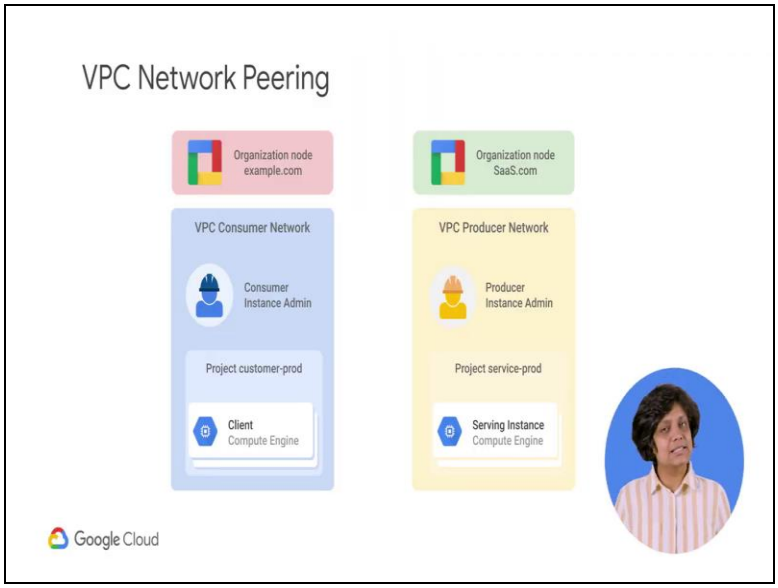
In this diagram there is one network that belongs to the web application service project. This network is shared with three other projects namely the recommendation service, personalization service and analytics service. Each of these service projects has instances that are in the same network as the web application server allowing for private communication to that server using internal IP addresses. The application server communicates with clients and on-premises using the service external IP address.

The back-end services on the other hand cannot be reached externally because they only communicate using internal IP addresses. When you use shared VPC you designate a project as a host project and attached one or more other service projects to it. In this case the web application

service project is the host project and the three other projects are the service projects. The overall VPC network is called the shared VPC network. VPC network pairing allows private RFC1918 connectivity across 2 VPC networks regardless of whether they belong to the same project or the same organization.

Now remember that each VPC network will have firewall rules that define what traffic is allowed or tonight between the networks.

(Refer Slide Time: 01:54)

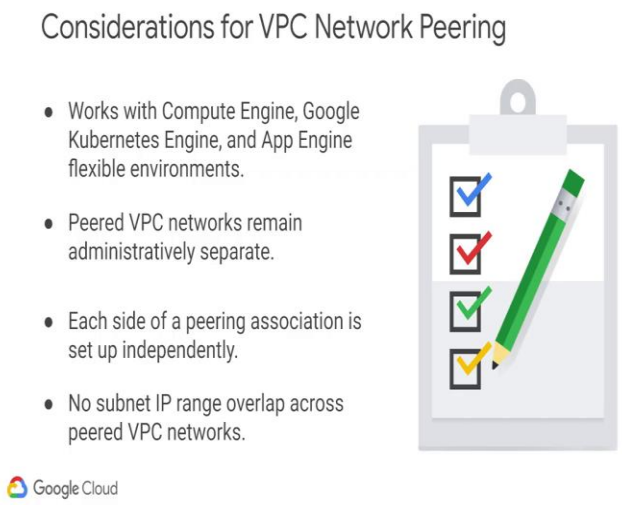


In this diagram there are 2 organizations that represent a consumer and producer respectively. Each organization has its own organization nodes, VPC network, VM instances, and network admin and instance admin. In order for VPC Network pairing to be established successfully the producer network admin needs to peer, the producer network with the consumer network. And the consumer network admin needs to peer, the consumer network with the producer network.

When both pairing connections are created the VPC network during session becomes active and routes are exchanged. This allows to VM instance has to communicate privately using their internal IP addresses. VPC Network pairing is a decentralized or distributed approach to multi-project networking. Because each VPC network may remain under the control of separate administrator groups and maintain its own Global firewall and routing tables.

Historically such projects would consider external IP addresses or VPN,s to facilitate private communication between BBC networks. However VPC network peering does not incur the network latency, security and cost drawbacks that are present when using external IP addresses or VPN's.

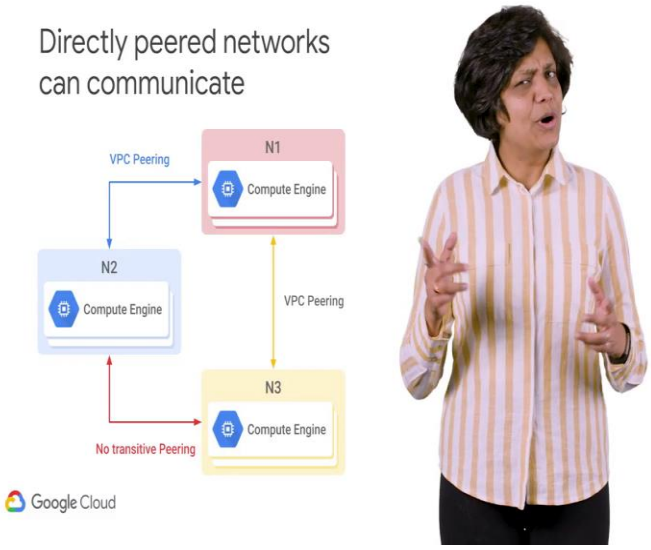
(Refer Slide Time: 03:22)



There are some things to remember when using VPC network peering. VPC Network peering words with compute engine Google kubernetes engine and app engine flexible environments. Peered VPC network remain administratively separate which means that route firewalls VPN's and other traffic management tools are administered and applied separately in each of the VPC network. Each side of peering association is set up independently.

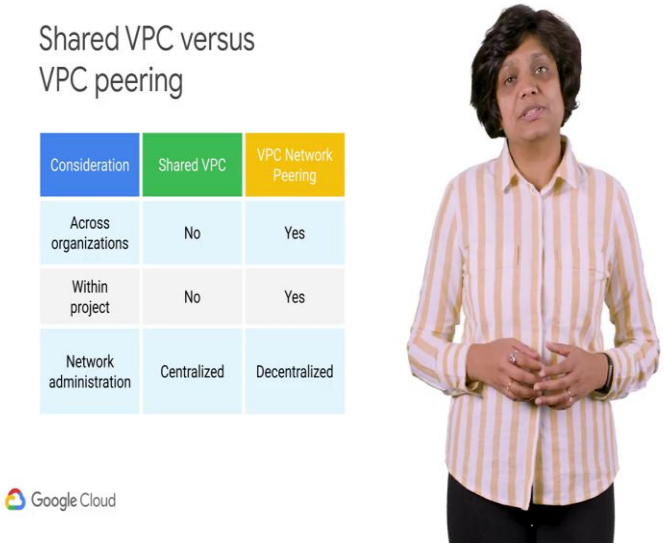
So, peering will be active only when the configuration from both sides match this allows either side to delete the peering association at any time. A subnet cyto prefix in one peered VPC network cannot overlap with a subnet cyto prefix and another peered network. This means that to auto mode VPC networks that only have the default subnet cannot pair.

(Refer Slide Time: 04:17)



There is one more thing to remember when using VPC network peering. Only peered networks can communicate meaning that the transitive peering is not supported in other words if VPC network M1 is filled with M2 and M3 but M2 and M3 are not directly connected. VPC Network M2 cannot communicate with the VPC Network M3 over the peer. This is critical if M1 is a software-as-a-service organization offering services to end to an end M3.

(Refer Slide Time: 04:50)



Now that you have learned about shared VPC and VPC network, let us compare both of these configurations to help you decide which is appropriate for a given situation. If you want to configure private communication between VPC networks in different organizations, you have to use VPC network peering. Shared VPC only works within the same organization. Somewhat

similarity if you want to configure private communication between VPC networks in the same project. You have to use VPC network peering.

This does not mean that the network needs to be in the same project, but they can be as you will explore in the upcoming lab. Shared VPC only works across projects. In a shared VPC The network administration is centralized. In a VPC Network peering situation the network administration is decentralized.