

**Google Cloud Computing Foundation Course**  
**Priyanka Vergardia**  
**Google Cloud**

**Lecture-58**  
**Building Hybrid Clouds**

**(Refer Slide Time: 00:05)**

Cloud VPN

- Useful for low-volume data connections
- 99.9% SLA
- Supports:
  - Site-to-site VPN
  - Static routes
  - Dynamic routes (Cloud Router)
  - IKEv1 and IKEv2 ciphers



In the next topic, you will learn how to build a hybrid Cloud using GCP. Cloud VPN securely connects on premise network to GCP, VPC Network through an IPSEC, VPN Tunnel. Traffic traveling between the two networks is encrypted by one VPN gateway then decrypted by the other VPN gateway. This protects data as it travels over the public internet and that is why Cloud VPN is useful for low-volume data connections.

As a managed service Cloud VPN provides an SLA of 99.9% service availability and support site-to-site VPN. Cloud VPN only support site-to-site IPSEC VPN connectivity. It does not support client to gateway scenarios. In other words Cloud VPN does not support use cases where client computer need to dial into a VPN using client VPN software. Cloud VPN; support sports static routes and dynamic route to manage traffic between VM instances an existing infrastructure.

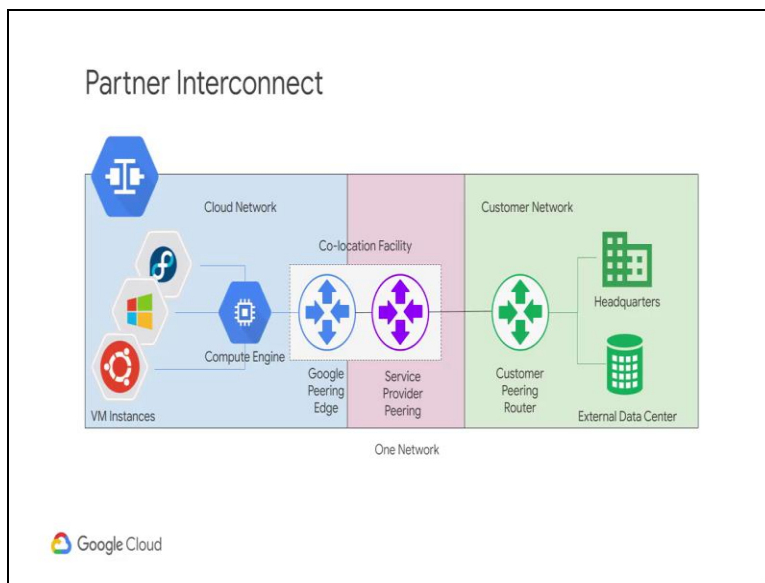
Dynamic routes are configured with Cloud router which you cover briefly both like version 1 and version 2 ciphers are also supported. Cloud interconnect provides 2 options for extending an on-premise network to a Google Cloud platform VPC Network.

**(Refer Slide Time: 01:27)**



Cloud interconnects dedicated also referred to as dedicated interconnect and Cloud interconnect partner also referred to as partner interconnect. Choosing an interconnect types will depend on connection requirements such as the connection location and capacity.

**(Refer Slide Time: 01:46)**



Dedicated interconnect provides direct physical connectivity between an organization's on-premise network and the Google Cloud Network Edge allowing them to transfer large amount of

data between networks, which can be more cost-effective than purchasing additional bandwidth over the public internet if 10 gigabytes per second or 100 gigabytes per second connections are not required. Partner interconnect provides variety of capacity options. Also, if an organization cannot physically meet Google's Network requirements in a colocation facility they can use partner interconnect to connect to a variety of service providers to reach their VPC networks.

Partner interconnect provides a service provider enables connectivity between an on-premise network and Google Cloud Network Edge allowing an organization to extend its private network into its Cloud Network. The service provider can provide solutions that minimize router requirements on the organization premises to only supporting an Ethernet interface to the cloud. Let us compare the interconnect options to considered all of these options provide internal IP address access between resources in an on-premise network and VPC Network.

**(Refer Slide Time: 03:10)**

A comparison of interconnect options

Connection	Provides	Capacity	Requirements	Access type
IPsec VPN tunnels	Encrypted tunnel to VPC networks through the public internet	1.5 - 3.0 Gbps per tunnel	On-premises VPN gateway	Internal IP addresses
Dedicated Interconnect	Dedicated, direct connection to VPC networks	10 Gbps per link	Connection in a colocation facility	Internal IP addresses
Partner Interconnect	Dedicated bandwidth, connection to VPC network through a service provider	50 Mbps – 10 Gbps per connection	Service provider	Internal IP addresses

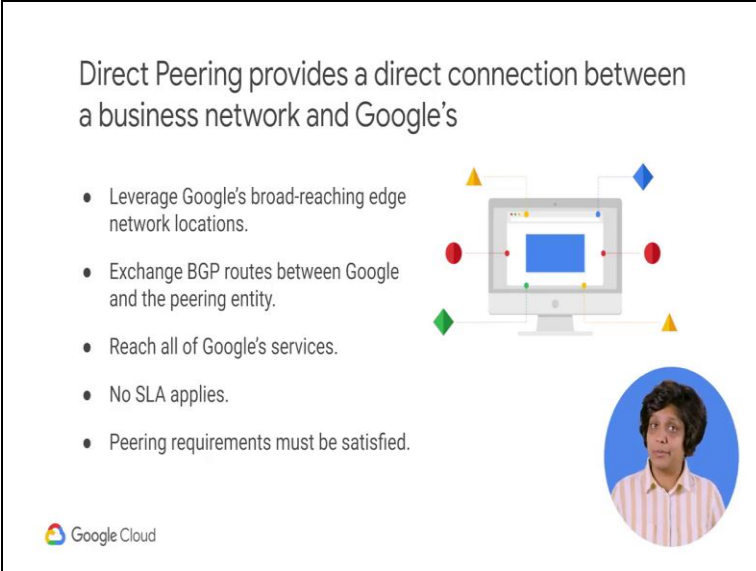


The main differences are the connection capacity and the requirements for using a service. The IPsec VPN tunnels that cloud VPN offers have a capacity of 1 and 1/2 to 3 GB per second for tunnel and require a VPN device on the on premise network. The 1 and 1/2 gigabyte per second capacity applies to traffic that traverses the public internet and the 3 gigabytes per second capacity applies to traffic that is traversing a direct peering link.

Configuring multiple tunnels allows you to scale this capacity. Dedicated interconnect has a capacity of 10 gigabytes per second per link and requires you to have a connection in the Google support at colocation facility. You can have up to 8 links to achieve multiples of 10 gigabytes per second, but 10 gigabytes per second is the minimum capacity. Partner interconnect has a capacity of 50 megabytes per second to 10 GB per second per connection.

And requirements depend on the service provider. The recommendation is just stop with VPN tunnels and depending on the proximity to a colocation facility and capacity requirements to switch to Dedicated interconnect or partner interconnect when there is a need for enterprise-grade connections to GCP.

**(Refer Slide Time: 04:31)**



Direct Peering provides a direct connection between a business network and Google's

- Leverage Google's broad-reaching edge network locations.
- Exchange BGP routes between Google and the peering entity.
- Reach all of Google's services.
- No SLA applies.
- Peering requirements must be satisfied.

Google Cloud

The slide features a central diagram of a computer monitor with several colored arrows (yellow, red, green, blue) pointing towards it from different directions, representing network connections. In the bottom right corner, there is a circular portrait of a man with dark hair wearing a striped shirt.

Google allows an organization to establish a direct peering connection between their business networks and ours. With this connection they will be able to exchange internet traffic between their network and ours at one of the Google's broad-reaching as network locations. Direct peering with Google is done by exchanging border Gateway protocol routes between Google and peering entity. And after a direct peering connection is in place they can use it to reach all of our services, including the full Suite of GCP products.

Unlike dedicated interconnect direct peering does not have an SLA. In order to use direct peering they need to satisfy the peering requirements. If an organization; requires access to Google

public infrastructure and cannot satisfy or peering requirements, they can connect through a carrier peering service provider.

**(Refer Slide Time: 05:25)**

Carrier Peering provides connectivity through a supported partner

- Leverage a provider's enterprise-grade network services to access Google applications.
- Get connections with higher availability and lower latency.
- No SLA offered by Google but may be offered by the provider.



Carrier peering enables them to access Google applications such as G Suite by using a service provider to obtain enterprise-grade Network Services that connect their infrastructure to Google. When connecting to Google to a service provider. They can get connections with higher availability and lower latency using one or more links. As direct peering Google does not offer an SLA with carrier peering but the network service provider might.

**(Refer Slide Time: 05:56)**

A comparison of peering options

Connection	Provides	Capacity	Requirements	Access type
Direct Peering	Dedicated, direct connection to Google's network	10 Gbps per link	Connection in GCP PoPs	Public IP addresses
Carrier Peering	Peering through a service provider to Google's public network	Varies based on partner offering	Service provider	Public IP addresses



Let us compare the peering options that you just considered. Both of these options provide public IP address access to all of our services. The main differences are capacity and the requirements for using a service. Direct peering has a capacity of 10 gigabytes per second for link and requires you to have a connection in a GCP edge point of presence. Carrier peering capacity and requirements vary depending on the service provider that you work with.