Google Transit VPC组网说明

liuchenggang@google.com
刘承罡

Google Cloud

术语对应: Google Cloud Interconnect

InterConnect对应的AWS服务: Direct Connection

Vlan Attachment 对应AWS VIF

提供私网地址的互联 (RFC1918)

混合云部署

不依赖硬件VPN设备

Dedicated interconnect

- 对应AWS DX Dedicated Connection
- 提供10G/100G的物理端口给客户

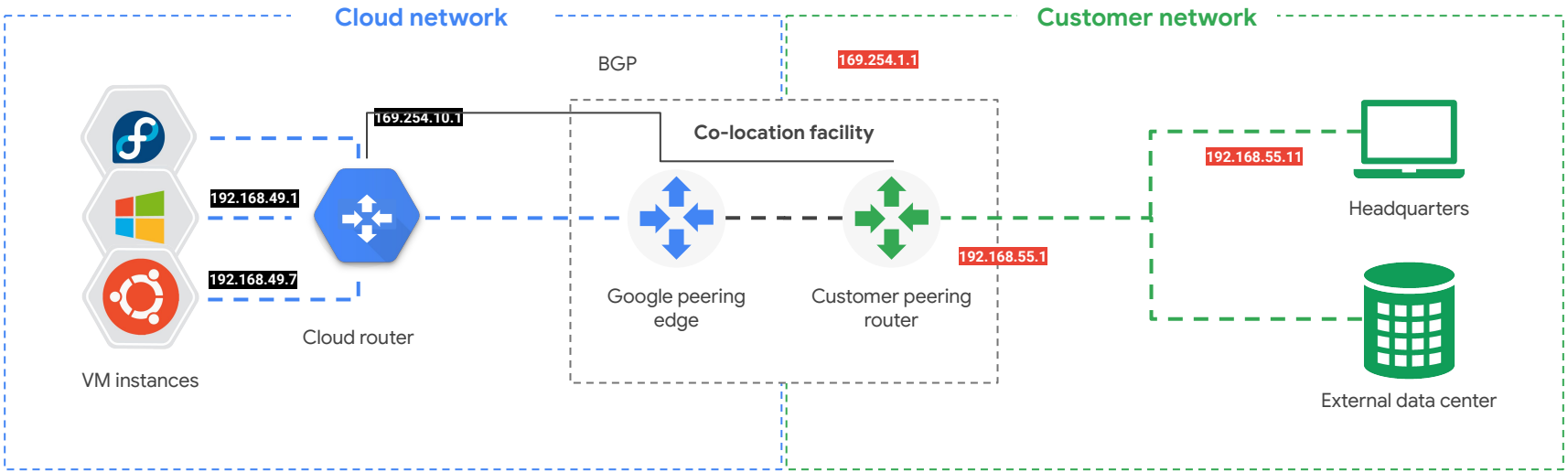
Partner interconnect

- 对应AWS DX Hosted Connection
- 提供(50Mbps - 50Gbps)的虚拟端口给客户

Google Cloud

术语对应: Cloud Router

- 在专线的场景中对应AWS的DX Gateway
- 和Customer Router或者SP Router做BGP连接



Google Cloud

术语对应: Cloud VPN + Cloud Router

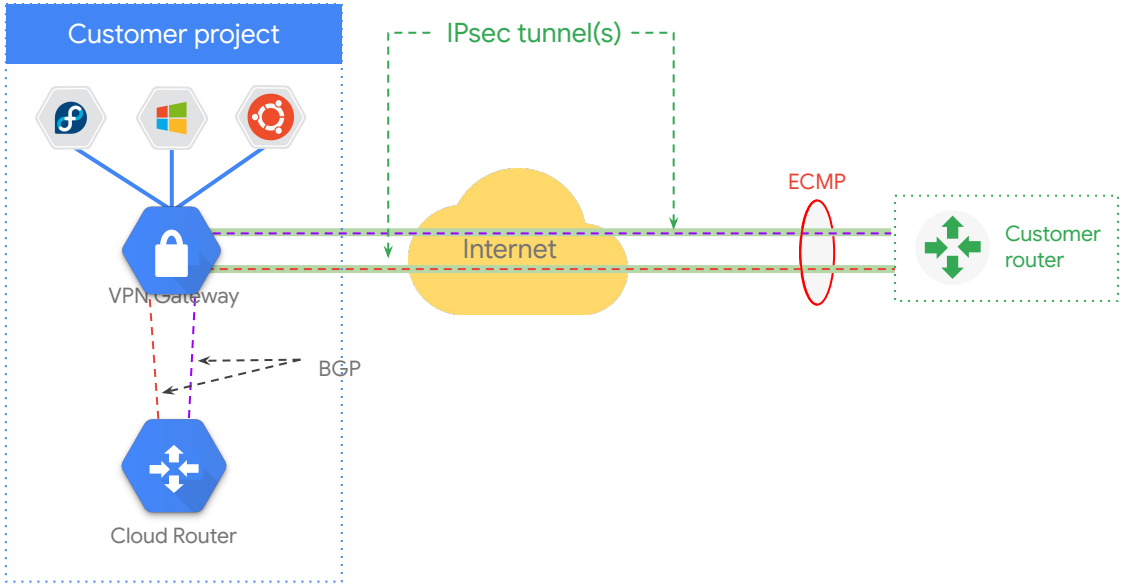
Cloud VPN和Cloud Router对应AWS的VPN Gateway,分别用来实现数据平面(IPSEC)和控制平面(BGP)

支持(RFC1918)的私网互联

支持通过Internet实现安全互联

通过IPSec 实现端到端的加密

每个Tunnel的最大带宽是3Gbps: 可以配置通过ECMP实现更大的出流量带宽



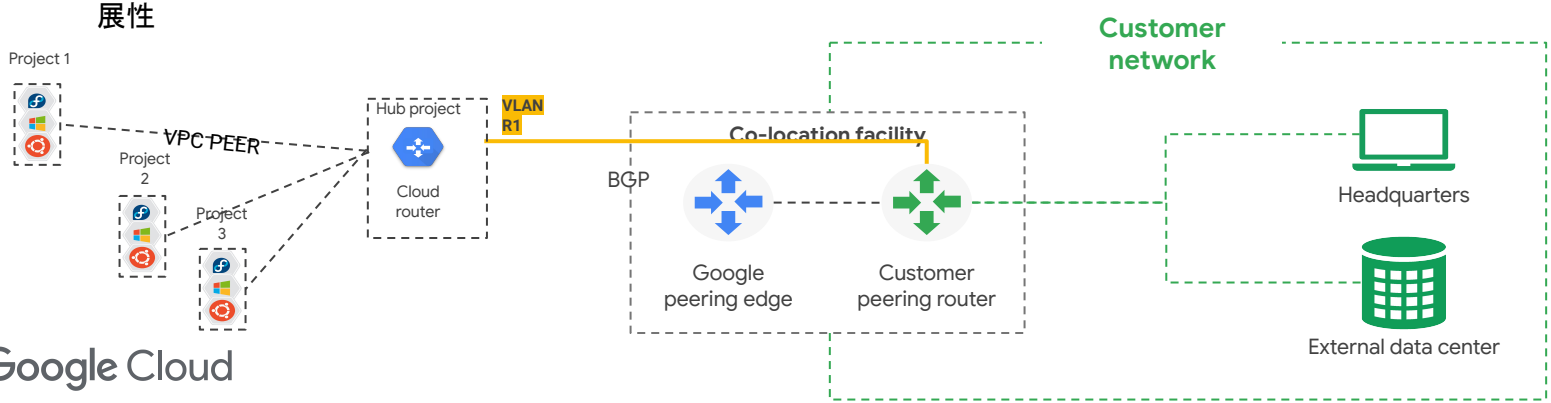
Guides for 3rd-party device configuration are available at:
https://cloud.google.com/compute/docs/vpn/interop-guides

如何在GCP环境上实现混合云网络方案?

- **低成本**: 流量成本, 端口成本,线路的成本
- **多项目支持**: 需要支持几十甚至几百个项目
- **灵活性**: 维护灵活,可以根据流量灵活的控制互联的类型和带宽,极可能少维护南北向的连接,南北向的高可用和SLA考虑
- **透明**: 账单清晰,每个项目的流量费计量计费清楚

通过Transit VPC实现Hub-Spoke

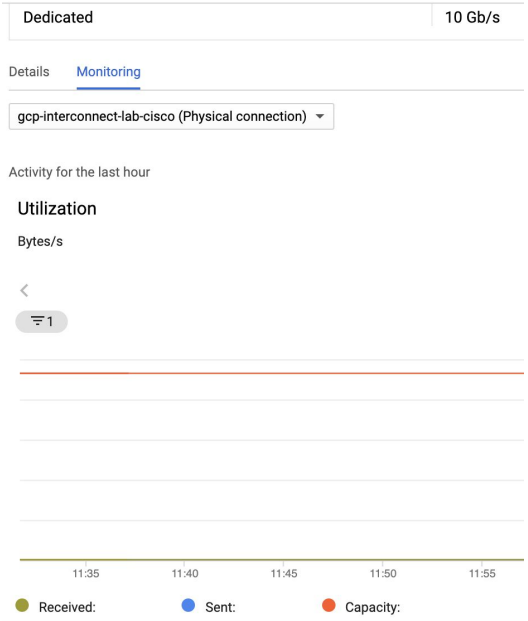
- 实现方式
  - 为Transit Project创建一个VLAN Attachment+Cloud Router和其他云环境实现BGP互联
  - 其他Project的Spoke VPC和所有的Transit VPC做Peering
  - Cloud Router通过自定义宣告把Spoke VPC的子网路由以及 private.googleapis.com的公网路由宣告 给对端
  - Transit VPC导出路由给所有Spoke VPC; Spoke VPC导入路由(on-premise和其他CSP路由)
- 优势:
  - 运维简单, 在一个点进行混合云BGP的构建
  - 成本低: 维护一对VLAN Attachment
- 缺点:
  - Hub VPC作为Peering的汇聚点最大支持和25个Spoke VPC做Peering,后期可以考虑结合Shared VPC来提高扩展性



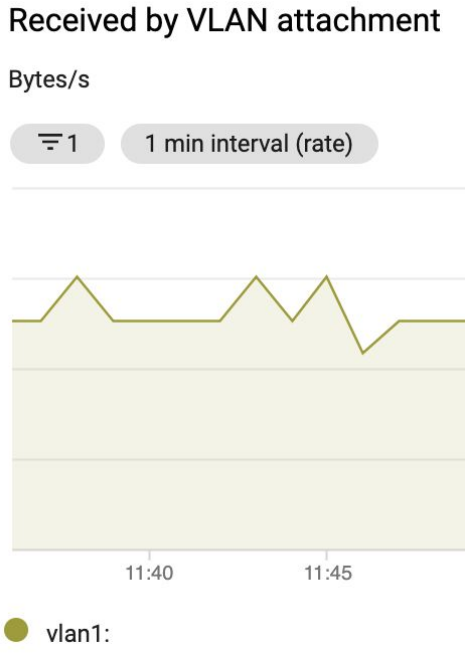
Google Cloud

对专线线路的监控

专线使用率

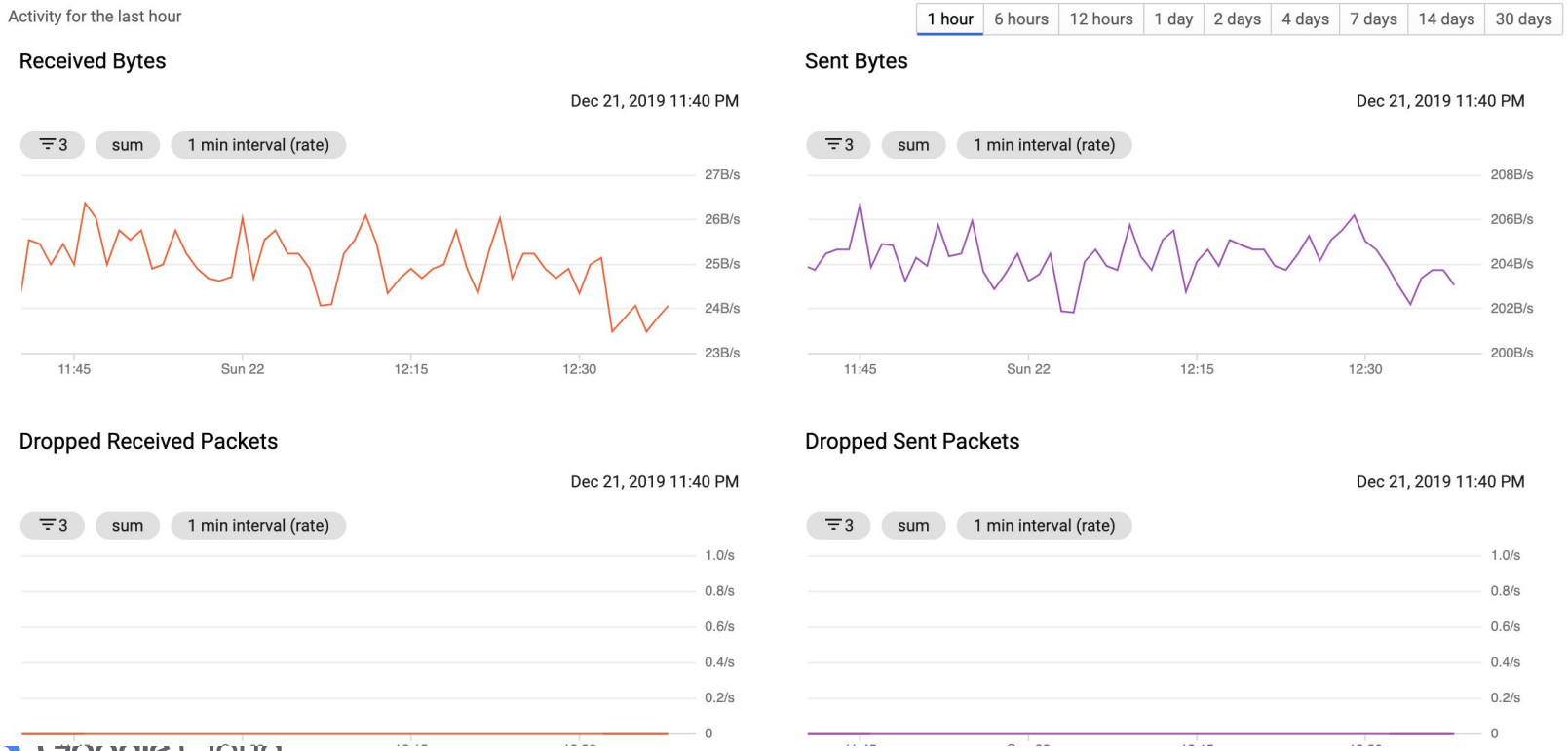


VLAN的接受吞吐



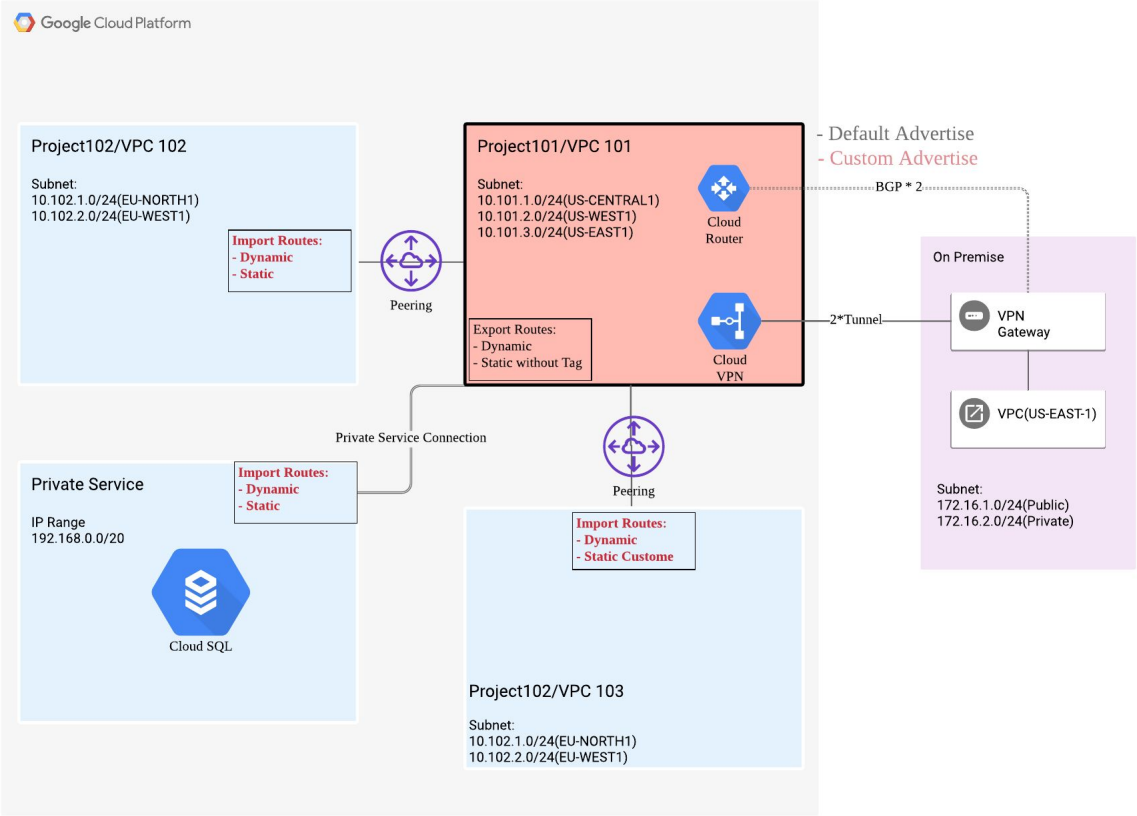
专线的错误率

VPN的监控



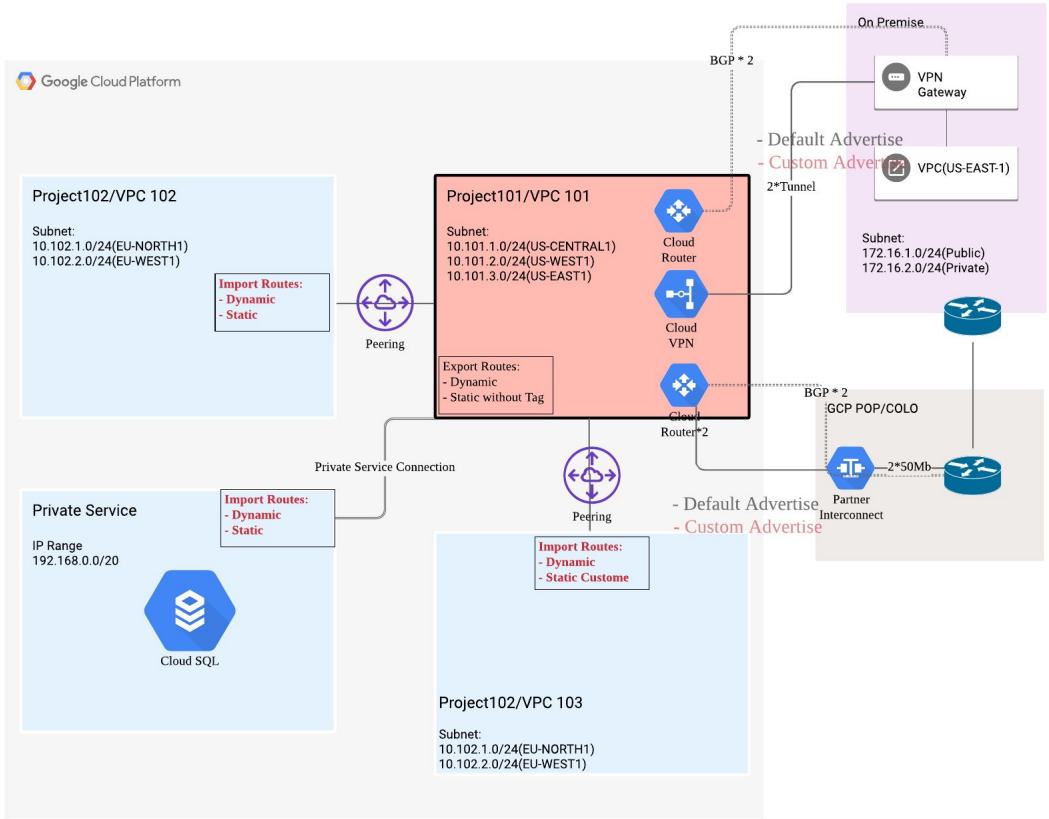
Google Cloud

初期构建网络架构图



- VPN方式和其他云/On Premise互联
- 通过Cloud Router 实现VPC101/On Premise BGP互联
- VPC101作为Transit VPC分别和VPC102/VPC103进行Peer
- 通过VPC Peer Export/Import把On Premise路由导出给VPC102/VPC103
- 通过Cloud Router Custom Advertise把VPC102/103子网路由宣告给On Premise
- 通过Cloud Router Custom Advertise把199.36.153.4/30; 199.36.153.8/30公网路由宣告给On Premise; 通过VPN访问Google API
- On Premise DNS上增加两条记录:CNAME: *.googleapis.com -> private.googleapis.com; A记录: private.googleapis.com 199.36.153.8/30

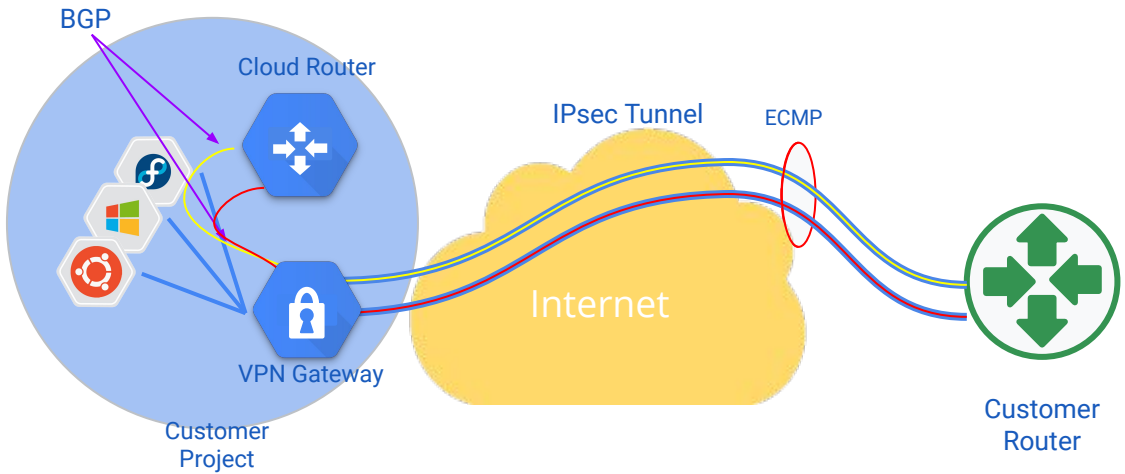
中期网络架构图



- 新增两条50MB的Partner Interconnect
- 在原有的Cloud Router上新增两个BGP Session,自定义MED值 = 1000 > VPN BGP MED
- BGP正常建立后, 修改VPN BGP MED =1000; VLAN BGP =100
- 最后的拓扑的2条专线为主线路; VPN为备用线路

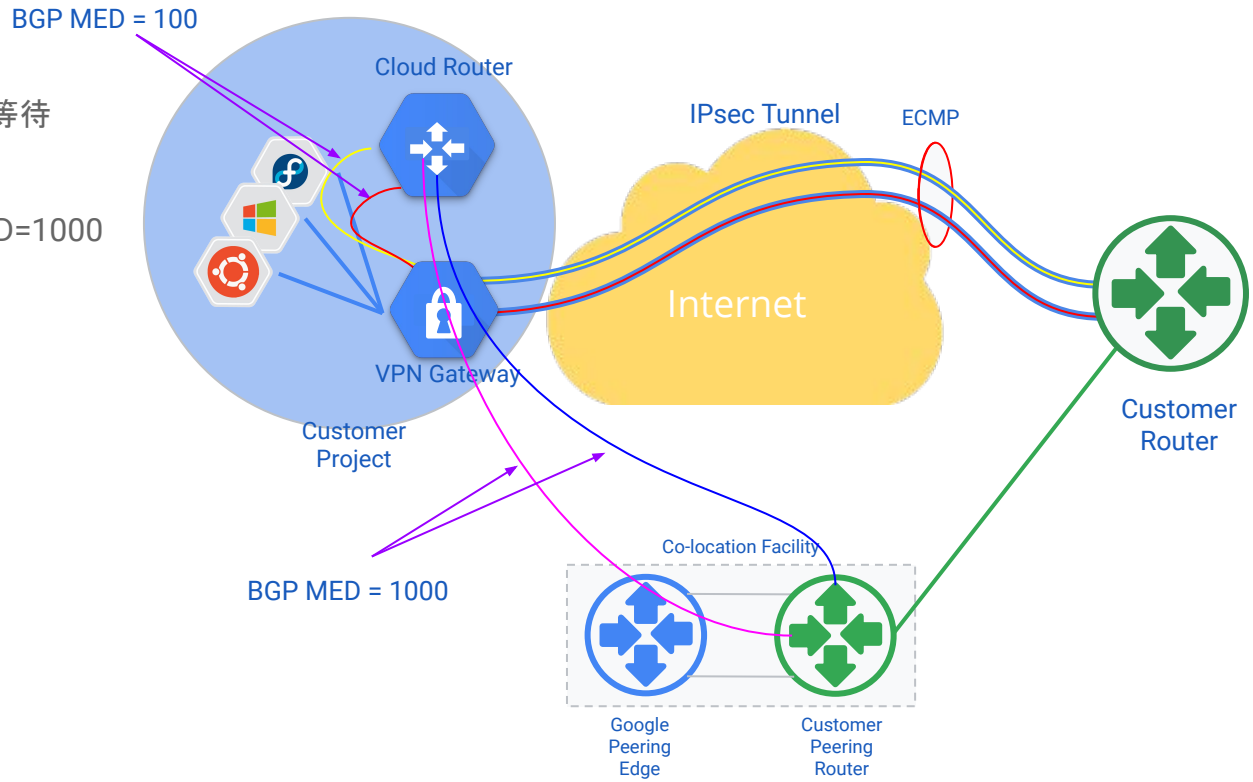
通过BEP MED对切换IPSec VPN到Interconnect

- VPN使用动态路由
- BGP MED 值使用默认值100



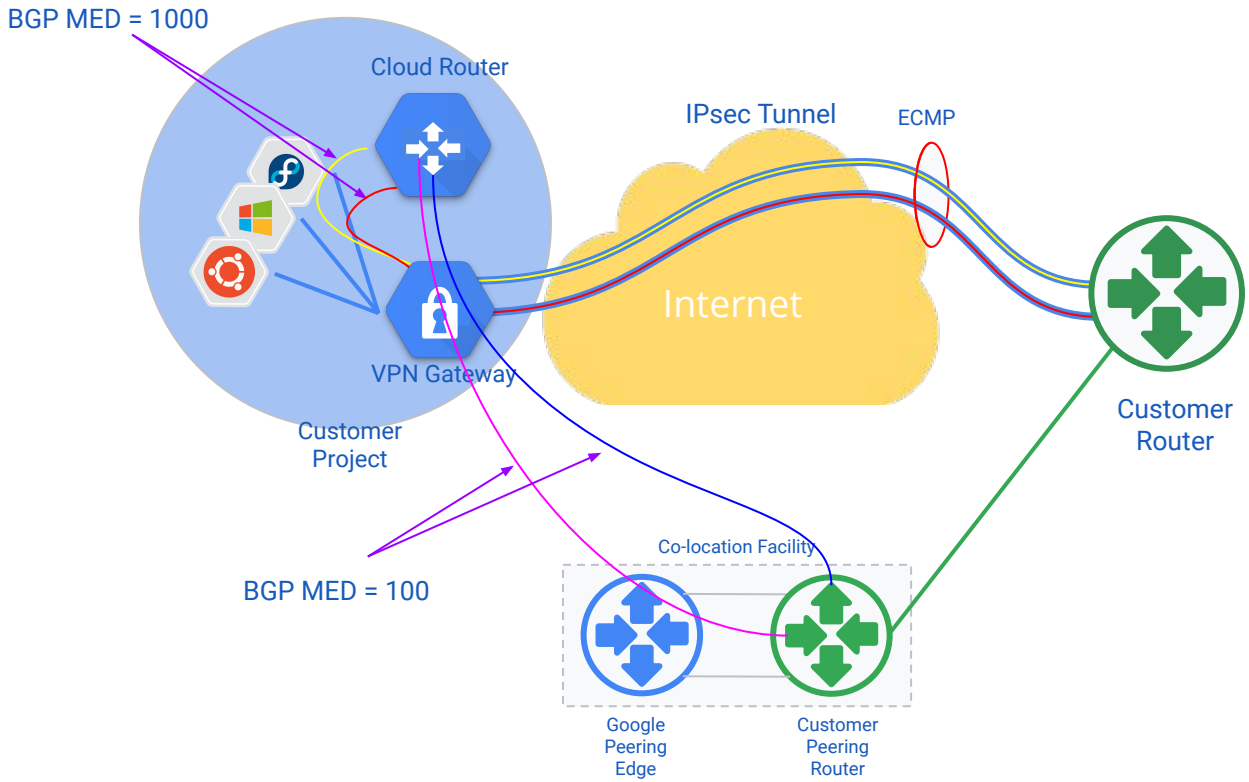
通过BEP MED对切换IPSec VPN到Interconnect

- 创建第二条InterConnect链路, 等待BGP 建立
- 设置InterConnect上的BGP MED=1000

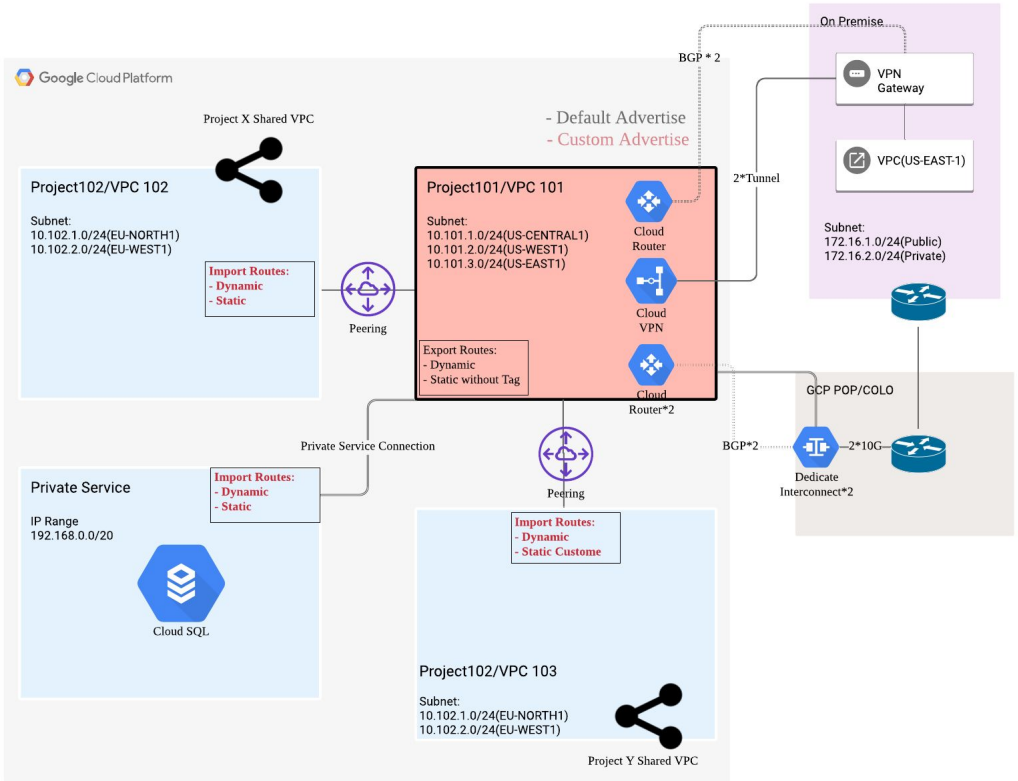


通过BEP MED对切换IPSec VPN到Interconnect

- 交换VPN和IC BGP上的MED值
- IC作为主线路
- VPN作为备用线路



远期网络架构图



- 专线无法在线扩展带宽,需要新建更高带宽的VLAN Attachement之后,通过修改MED值得方式把流量切换到新的高带宽专线上
- 目前每个POP点支持的最大带宽是10*8GB or 100GB*2
- 25个SpokeVPC的Limit到达后,可以通过在Shared VPC对Transit VPC/Spoke VPC网络进行扩展

GCP年费用预估($)

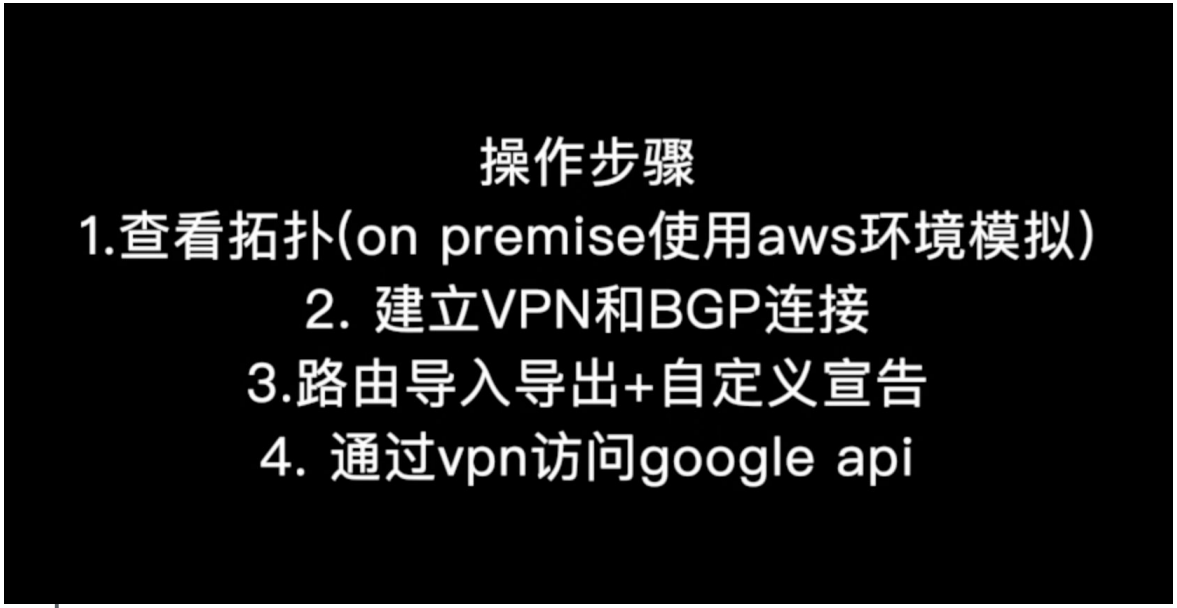
1. DX端口占用费(20个Project需要通过Transit VPC共享一对50Mb的Parnter InterConnection: 87960*2*0.05417 = **9529**
2. 专线出方向流量费(美国/欧洲/亚洲各10TB): 0.0491*101000 + 0.06*10000 + 0.041*10000 = **5,969**
3. 云中跨区域流量费用: 3*2*10000*0.08 = **4800**
4. 备用VPN费用: 0.05*87960*2= **8796**

合计: 29,094

Google Cloud

Demo配置视频

混合云Transit VPC配置.mp4



Google Cloud

Thank you

Google Cloud