This reference architecture provides generic guidance for an asset light Provider deploying multi-tenant customers in VMware Cloud Director service with Google Cloud VMware Engine. All networking information depicted here is generic examples and can be customized for the Provider’s needs.

1. **Tenant connectivity** for workload access.
   - Provider will create VPN in tenant’s project and create an IPsec tunnel to tenant’s Tier1 Gateway.
   - Tenant connects to their project via Google Cloud Cloud VMware Engine connection or interconnect.
   - Otherwise, tenant access to workloads will be via the tenant portal VM console.

2. **Internet connectivity** for workload and tenant access.
   - There are several options for the tenant to choose from for default routing to the Internet.
     - Tenant A does not have their own GCP project and has opted for provider provided Internet, so the default route is leaving the provider managed consumer project via an ILB.
     - Tenant B has their own GCP project and has opted to manage their own Internet, so default route is to their project, then routes via an ILB in their project.
     - A tenant could also route all traffic to their on-prem location and traffic egress from there.
   - Provider will create allow rules on the Compute Gateway to allow inbound and outbound traffic from Tier1 Gateways.
   - Tier1 Gateway firewall rules will govern access to tenant workloads.

3. **Internet Load Balancers** for Internet workload traffic.
   - The incoming traffic will likely ingress in GCP via either:
     - Tenant A has opted for provider managed ILBs.
     - Tenant B has opted to host ILBs in their on GCP project.

4. **NAT Rules** for workload and tenant access.
   - Provider will allocate public IPs in GCP console and NAT to the external network IP of the tenant.
   - Tier1 Gateway will provide NAT of the external IP to the internal IP of the tenant segment.

---

**Tenant A (On-Prem)**

- **Tenant Portal**
- **Tenant Cloud Admin**
- **Application Workload**
- **End Users**

**Tenant A VPC (Provider owned customer project)**

- **Firewall Rules (On-Prem Router)**
  - Source: 172.28.4.0/24
  - Destination: 172.28.8.0/24
  - Protocol: TCP

**Tenant B (On-Prem)**

- **Tenant Portal**
- **Tenant Cloud Admin**
- **Application Workload**
- **End Users**

**Tenant B VPC (Provider owned customer project)**

- **Firewall Rules (On-Prem Router)**
  - Source: 172.28.7.0/24
  - Destination: 172.28.8.0/24
  - Protocol: TCP

**Tenant B VPC (Customer owned project)**

- **Firewall Rules (On-Prem Router)**
  - Source: 172.28.7.0/24
  - Destination: 172.28.8.0/24
  - Protocol: TCP

---

©2020 VMware, Inc. - Designed by the Cloud Provider Software Technical Product Management team
This reference architecture provides generic guidance for an asset light Provider deploying multi-tenant customers in VMware Cloud Director service with Google Cloud VMware Engine. All networking information depicted here is generic and can be customized for the Provider’s need.

**Provider Connectivity**
- IPsec VPN (Google Cloud VPN) or Interconnect between Provider on-prem datacenter and Provider project on GCP.
- Policy-based VPN: Subnets have to be declared on both sides during the setup. One tunnel is created per subnet. It is recommended to use large subnets.
- Route-based VPN: Subnets are automatically advertised through BGP. BGP configuration is mandatory, no static route can be configured on GCVE side.

**VPC Connectivity**
- This allows connectivity to the provider VPC from the customer owned VPC or the provider managed customer VPC.
- There are several connectivity options for the provider VPC to tenant VPC: VPC peering, Interconnect or Cloud VPN are all valid options whether the project is customer owned or provider owned customer project.
- Tenant A does not have its own GCP project, the provider could setup VPC connectivity through Google Cloud VPN or Interconnect.
- Tenant B has its own GCP project and has decided to use VPC peering.

**Private Service Connect**
This will allow connectivity from the Provider or the customer project to services leveraging Google Native Services (Storage Bucket, Filestore, BigQuery, Google Cloud SQL, etc.) and traditional Virtual Machines to application workloads.
- Allow access from/to VPC subnets and External Network segments in the Compute Gateway and through IPsec VPN and Firewall Rules.

**Infrastructure VMs**
Deploying infrastructure VMs inside GCVE is recommended to provide reliability and performance to application workloads.
- Usual infrastructure components are (but not limited):
  - Active Directory (RDOC might be considered)
  - DNS Server
  - Backup Server

**DNS Configuration**
Tenant workloads should use Tier 1 Gateway DNS
- Provider can configure Tier 1 Gateway DNS forwarder to use custom DNS server.

**Customer Managed**
- The customer owned GCP project is managed by the customer.
- Customer will be required to setup connectivity to/from other VPCs themselves with information supplied by provider.

©2020 VMware, Inc. – Designed by the Cloud Provider Software Technical Product Management team
This reference architecture provides a generic guidance to start deploying VMware Cloud Director service with Google Cloud VMware Engine as a multi-tenant solution accessed by customer end-users. All networking information depicted here is generic examples and can be customized as per provider’s need.

1. **On-Prem connectivity**
   - **Ipsec VPN** (Google Cloud VPN) or Interconnect between Provider on-prem datacenter and Provider project on GCP.
     - Policy-based VPN: Subnets have to be declared on both sides during the setup. One tunnel is created per subnet. It is recommended to use large subnets.
     - Route-based VPN: Subnets are automatically advertised through BGP. BGP configuration is mandatory, no static route can be configured on GCVE side.

2. **Firewall rules**
   - **For vCenter Access.**
     - If On-Prem connectivity is configured, allow infrastructure on-prem subnets to access vCenter & ESXi (allowing remote console, vMotion and possibly Hybrid Linked Mode).
     - Otherwise, access can be allowed from public Internet but it is highly recommended to limit it to few trusted public IPs (not detailed here).

3. **On-Prem Firewall**
   - Access from on-prem subnets to GCVE Management segment (or at least vCenter and ESXi).
   - Access from GCVE vCenter to on-prem infrastructure services (Active Directory, DNS, Content Library, ...)

4. **Routed Network Segments**
   - One Infrastructure segment with privileged access to Management components (vCenter, NSX, ...)
   - One or multiple workload segments where all the applications VMs will be deployed.

5. **Firewall rules for Network segments**
   - Allow connectivity between Infra & Management
   - Allow connectivity between Infra & on-prem infrastructure subnet
   - Allow connectivity between workload segment, GCP VPC Subnets and on-prem application subnets

6. **Infrastructure VMs**
   - Designing infrastructure VMs inside GCVE is recommended to provide reliability and performance to application workloads.
   - Usual infrastructure components are (but not limited):
     - Active Directory (BDC might be considered)
     - DNS Server
     - Backup Server

7. **DNS Configuration**
   - GCVE Compute Gateway should use on-prem DNS servers (applications can resolve enterprise domains)
   - vCenter alias to resolve using its private IP (allowing access from on-prem through its alias)

8. **VPC connectivity**
   - VMs will be able to create hybrid applications leveraging Google Native Services Storage Bucket, Filestore, BigQuery, Google Cloud SQL, etc., and traditional Virtual Machines.
   - Allow access from/to VPC subnets and Workload segments in the Compute Gateway and Security Groups.

9. **ASN heavy Provider Model**
   - Providers selling VMware Cloud on AWS with their own branded extended service offering.
   - The reference architecture provides a generic reference architecture that can be customized as per provider’s needs.

10. **Google Cloud VMware Engine**
    - This will allow to create hybrid applications leveraging Google Native Services Storage Bucket, Filestore, BigQuery, Google Cloud SQL, etc., and traditional Virtual Machines.
    - Allow access from/to VPC subnets and Workload segments in the Compute Gateway and Security Groups.

---

©2020 VMware, Inc. - Designed by the Cloud Provider Software Technical Product Management team