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

1. **Tenant connectivity** for workload access.
   - Customer will create VPN in their compartment DRG and create an IPsec tunnel to their Tier1 Gateway.
   - Otherwise, tenant access to workloads will be via the tenant portal VM console.
   - Tenant's will gain access to their specific domains.

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 is using the Tier1 gateway for Internet. RFC 1918 traffic is routed via IPsec VPN.
     - Tenant B is routing traffic to their on-prem location and traffic egresses from there. Default route for all traffic is via IPsec VPN.
     - Tenant C can use the Tier1 gateway for Internet. RFC 1918 traffic is routed via IPsec VPN.
   - Provider will create allow rules on the Compute Gateway to allow inbound and outbound traffic from Tier1 Gateways.

3. **NAT Rules** for workload and tenant access.
   - Provider will allocate public IPs in OCI 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.

## Network Architecture

### Tenant A (On-Prem)
- **Tenant Portal**
- **Tenant Cloud Admin**
- Application Workload
- **End Users**

### Tenant A VCN (Customer owned)
- **Domain 1**
- **Domain 2**
- **Domain 3**

### Tenant B (On-Prem)
- **Tenant Portal**
- **Tenant Cloud Admin**
- Application Workload
- **End Users**

### Tenant B VCN (Customer owned)
- **Tenant A Segment**
- **Tenant B Segment**

### Tenant C (On-Prem)
- **Tenant Portal**
- **Tenant Cloud Admin**
- Application Workload
- **End Users**

### Tenant C VCN (Customer owned)
- **Domain 1**
- **Domain 2**
- **Domain 3**

---

©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 Oracle Cloud VMware Solution 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**
   - P2V WVD or FastConnect 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 OCI side.

2. **Firewall rules for Center 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. **Routing Network Segments**
   - One Infrastructure segment with privileged access to Management component (vCenter, NSX, …)
   - One or multiple workload segments where all the applications VMs will be deployed.

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

5. **VCN Connectivity to OCVS**
   - Connectivity from OCVS to the provider VCN is direct to the VCN via the Tier 0 NSX edge uplinks.

6. **Firewall Rules (On-prem Ruter)**

   - **Source**:Not Jumplead
   - **Destination**:Not Jumplead
   - **Protocol**:TCP, UDP

7. **Firewall Rules (SDDC Gateways)**

   - **Source**:Not Jumplead
   - **Destination**:Not Jumplead
   - **Protocol**:TCP, UDP