This reference architecture details how a Managed Service Provider can deploy VMware Cloud Director service with VMware Cloud on AWS to host multi-tenant workloads.

All networking information depicted here is generic and can be customized for the Provider's needs.

1. **Provider connectivity**
   - IPsec VPN (preferably route-based) or Amazon Direct Connect between Provider on-prem datacenter and VMC on AWS.
   - Policy-based VPN: Subnets must 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 VMC side.

2. **Tenant connectivity**
   - Provider will deploy a VPN server in the tenant Org and configure it for tenant access by assigning a public IP in VMC.
   - Otherwise, tenant access to workloads will be via the tenant portal VM console.

3. **Internet connectivity for workload access**
   - Provider will create allow rules on the Compute Gateway to allow inbound and outbound traffic from Tier 1 Gateways.
   - Tier 1 Gateway firewall rules will govern access to tenant workloads.

4. **NAT Rules for workload and tenant access**
   - Provider will allocate public IPs in VMC console and configure it for tenant access by assigning a public IP in VMC.
   - NAT to 10.0.1.0/24

5. **VPC connectivity**
   - This will allow the Provider to expose services leveraging Amazon Native Services (EC2 & RDS instances, S3 Buckets, EFS, etc.) and Traditional Virtual Machines to tenants.
   - Allow access from/to VPC subnets and External Network segments in the Compute Gateway and through Security Groups.

6. **Infrastructure VMs**
   - Deploying infrastructure VMs inside VMC 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

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

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