

This diagram shows how to design multi-site tenant networking on a cloud platform powered and managed by VMware Cloud Director (VCD) 10.3.

This solution can be utilized by service providers who want to reduce management overhead of complex tenants routing and networking, when each tenant has multiple assets across multiple locations.

- 1

Provider should configure a Virtual Routing and Forwarding (VRF) instance on their physical networking infrastructure for each tenant per location. A dedicated VRF will be used for internet access in each location as well. Tenant VRFs in each location must be fully routed to each other and to tenant-specific external assets like on-prem site(s) through WAN or hyperscale cloud environments, etc. Route filters are applied to exchange tenant's routes only and deny any other routes, including default route and public subnets.
- 2

For each tenant in each location, a dedicated NSX TO gateway will be deployed and connected to the tenant's physical VRF. BGP routing will be configured on this TO gateway to peer with the tenant's physical VRF. This TO gateway will act as a route aggregator and will be managed by the provider.

The provider can deploy these route aggregator TO gateways as NSX-T TO light VRFs and even leverage EVPN feature, if desired. However for maximum performance and throughput, we recommend deploying each route aggregator as a separate TO gateway. These route aggregator TO gateways can be part of the NSX environment managed by VCD or part of a separate NSX environment managed by VCD or part of a separate NSX environment managed by VCD or part of a separate NSX environment managed by VCD.

These route aggregator TO gateways can be part of the NSX environment managed by VCD or part of a separate NSX environment managed by VCD or part of a separate NSX environment managed by VCD or part of a separate NSX environment managed by VCD.
- 3

The tenant's assets in each location will be connected and routed to the tenant's route aggregator using either uplink VLANs or overlay logical switches. Physical resources and networking services will be routed to the route aggregator over uplink VLANs. Tenant-dedicated TO gateways in VCD will be routed to the route aggregator over NSX segments only if the same NSX Manager is managing both the tenant-dedicated TO gateways and the tenant's route aggregator TO gateway. Otherwise, routing will be over uplink VLANs. Specific route filters must be applied to allow exchanging tenant-specific routes and denying any other routes, including the default route and location-specific public subnets, to prevent exposing these networks over WAN links.
- 4

In each location, a separate TO gateway will be created to act as an internet route aggregator. The tenants' dedicated TO gateways under VCD will be connected and routed to the internet aggregator TO gateway. Tenants can manage internet access to workloads deployed under VCD in a self-service fashion using NAT rules on Org Edges. Provider can monitor and implement security and bandwidth controls as needed through the internet route aggregator TO gateway and the above layers. Specific route filters must be configured to allow exchanging only public subnets routes and the default route through the internet route aggregator TO gateway and deny any tenant-specific routes to be exchanged to prevent exposing the tenant's private subnets to the internet aggregator.

Legend:

VLAN Uplink / BGP

Overlay or VLAN Uplink / BGP

