This reference architecture provides generic guidance for an asset-light Provider deploying multi-tenant customers in VMware Cloud Director service with Azure 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 ExpressRoute connection from Azure VMware Solution to VmHs.
   - Customer creates NSX in VmHs traffic from ExpressRoute into VmHs as required for isolation.
   - Tenant on-prem connects to their VmHs via VPN Gateway connection to ExpressRoute.
   - Customer can deploy jumphost in Azure and access workloads via KDP or SSH.
   - Otherwise, tenant access to workloads via a tenant portal VM service.
   - Non-overlapping network behind T1 tenant for fully routable environments. Overlapping space behind T1 is supported as long as its not routable beyond the T1 and DMZs are used.

2. **Internet connectivity** for workload and tenant access:
   - Options for the tenant to choose from for default routing to the Internet:
     - Tenant A leverages the ExpressRoute connection to their own Azure Vnet for Internet, so the default route is via ExpressRoute.
     - Tenant B & C opting for a private IP or their Tier 1 edge for Internet, so the default route is via the Tier 1. A public and private IP is allocated to Tier 1 with the public IP providing outbound Internet while the private IP is for tenant to tenant communication.
     - Provider or tenant can create rule to access the Tier 2 gateway to allow inbound and outbound traffic from tenant workloads.

3. **Internet Load Balancers** for Internet workload traffic:
   - Currently only Layer 7 LB is supported by Azure LB in Azure VMware Solution for tenant workloads.

4. **NAT Rules** for workload and tenant access:
   - Customer will allocate public IPs in the tenant subscription and NAT to the internal network IP of the tenant workload.
   - Tenant’s gateway will provide NAT of the external IP to the internal IP of the tenant segment.

5. **Private Endpoint**:
   - This will allow connectivity to services leveraging Azure Native Services (Azure Blob Storage, Azure File Storage, Azure Synapse Analytics, etc.) and traditional SaaS/Mashup/externals to tenants.
   - Allows access from Tier 1 subnet and external network segments (split the Compute Gateway and through IPsec VPN and Firewall Rules).
   - Tenant A Tier1 Gateway firewall rules will govern access to tenant workloads.
   - Tenant A Tier1 Gateway firewall rules will govern access to tenant workloads.
   - Tenant A Tier1 Gateway firewall rules will govern access to tenant workloads.
   - Tenant A Tier1 Gateway firewall rules will govern access to tenant workloads.

6. **Infrastructure VmNs**:
   - Displaying of infrastructure VmNs inside Azure VMware Solution is recommended to provide reliability and performance to application workloads.
   - Usual infrastructure components are (but not limited):
     - Active Directory (RODC might be considered)
     - DNS Server
     - Backup Server

---

©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 Azure 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
   - (Firewall or ExpressRoute between VPC on-prem datacenter and customer VNet)
   - 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, on static route can be configured on Azure VMware Solution side.

2. Firewall rules for “Center Access”
   - If on-prem connectivity is configured, allow infrastructure on-prem subnets to access (Center & ESXi) (Allowing remote consoles, vMotion and possibly vMotion Link Mode)
   - Otherwise, access can be allowed from public Internet but it is highly recommended to limit to few trusted public IPs (not detailed here)

3. On-prem Firewall
   - Access from on-prem subnets to Azure VMware Solution Management segment (or on-prem (Center and ESXi)
   - Access from Azure VMware Solution(on-prem infrastructure services) (Active Directory, DNS, Content Library, etc.)

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

5. Firewall rules for networking segments
   - Allow connectivity between (infra & Management)
   - Allow connectivity between (infra & on-prem infrastructure subnet)
   - Allow connectivity between workload segment, VNs and on-prem application subnets

6. Infrastructure VNI
   - Deploying infrastructure VNIs inside Azure VMware Solution is recommended to provide reliability and performance to application workloads.
   - Usual infrastructure components are (but not limited to):
     - Active Directory (BODC might be considered)
     - DNS Server
     - Backup Server
   - DNS Configuration
     - Tenant workloads should infrastructure DNS or Azure DNS

7. Private Endpoint
   - This will allow connectivity from the Provider or the customer subscription to services leveraging Azure Native Services (Azure Blob Storage, Azure File Storage, Azure Synapse Analytics, etc.) and traditional Virtual Machines (VMs)
   - Allow access from VNet subnets and external Network segments in the Compute Gateway and through Firewalls/Rules.

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