

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 VNets.
- Customer creates NSGs to filter traffic from ExpressRoute into VNets as required for isolation
- Tenant on-prem connects to their VNet via VPN Gateway connection or ExpressRoute.
- Customer can deploy jump host in Azure and access workloads via RDP or SSH
- Otherwise, tenant access to workloads will be via the tenant portal VM console.
- Non-overlapping networks behind T1 in tenant for fully routable environment. Overlapping space behind T1 is supported as long as it is not routable beyond the T1 and DNATs 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 opted for a public IP on their Tier 1 edge for Internet, so the default route is via the Tier 1. A public and private IP is allocated per Tier 1 with the public IP providing outbound Internet while the private IP is for tenant to tenant communication.

- Provider or tenant will create allow rules on the Tier 1 gateway to allow inbound and outbound traffic from tenant workloads.
- Tier1 Gateway firewall rules will govern access to tenant workloads.

**3 Internet Load Balancers** for Internet workload traffic

- Currently only Layer 7 LB is supported by Azure LB in Azure VNet for tenant workloads

**4 NAT Rules** for workload and tenant access.

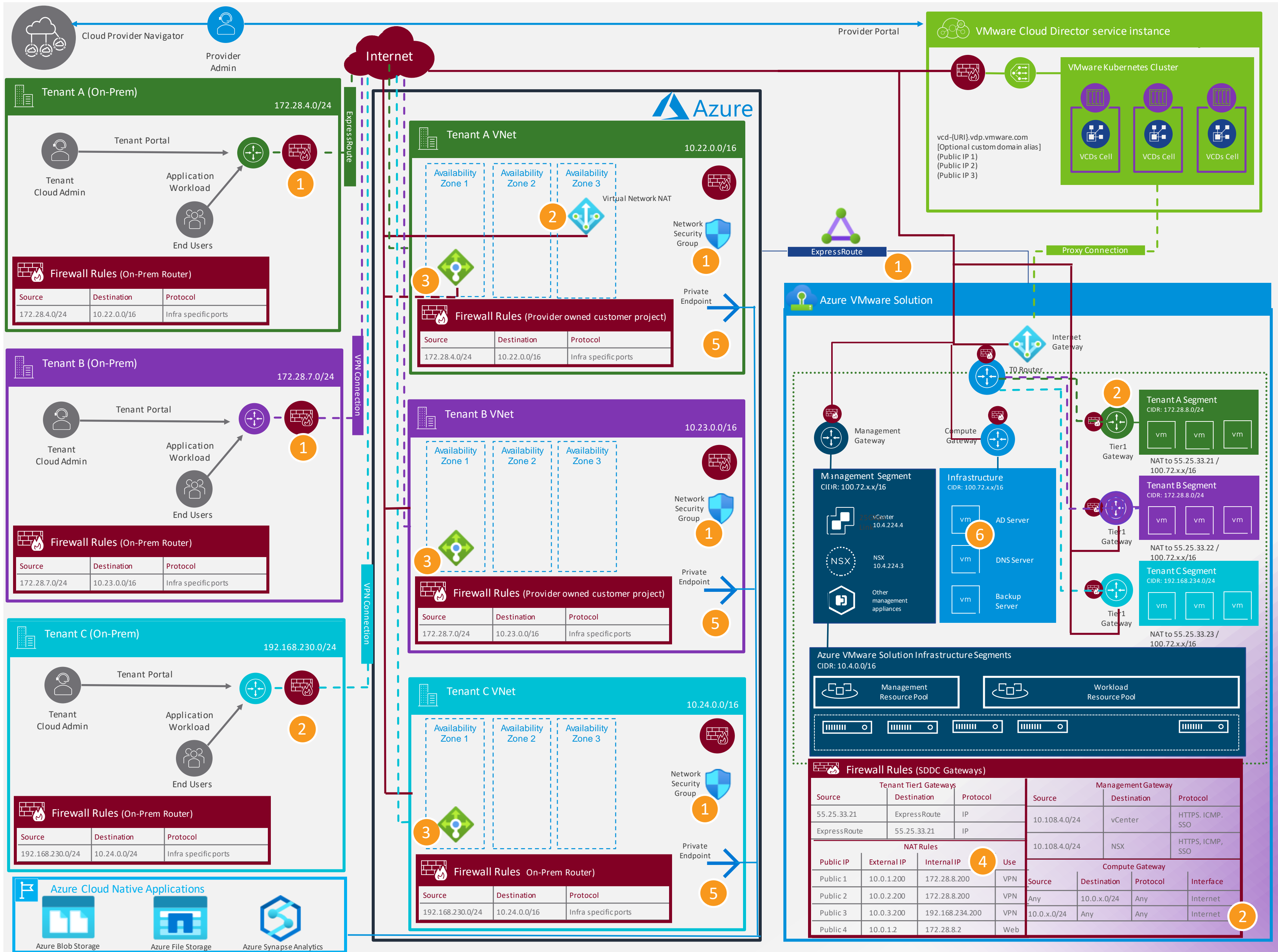
- Customer will allocate public IPs in tenant's subscription and NAT to the internal network IP of the tenant workload.
- Tier1 Gateway will provide NAT of the external IP to the internal IP of the tenant segment.

**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 Virtual Machines to tenants
- Allow access from/to VNet subnets and External Network segments in the Compute Gateway and through IPsec VPN and Firewall Rules.

**6 Infrastructure VMs**

- Deploying infrastructure VMs 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



**Tenant A (On-Prem)** 172.28.4.0/24

Tenant Cloud Admin, Application Workload, End Users

Source	Destination	Protocol
172.28.4.0/24	10.22.0.0/16	Infra specific ports

**Tenant B (On-Prem)** 172.28.7.0/24

Tenant Cloud Admin, Application Workload, End Users

Source	Destination	Protocol
172.28.7.0/24	10.23.0.0/16	Infra specific ports

**Tenant C (On-Prem)** 192.168.230.0/24

Tenant Cloud Admin, Application Workload, End Users

Source	Destination	Protocol
192.168.230.0/24	10.24.0.0/16	Infra specific ports

**Tenant A VNet** 10.22.0.0/16

Availability Zone 1, Availability Zone 2, Availability Zone 3

Source	Destination	Protocol
172.28.4.0/24	10.22.0.0/16	Infra specific ports

**Tenant B VNet** 10.23.0.0/16

Availability Zone 1, Availability Zone 2, Availability Zone 3

Source	Destination	Protocol
172.28.7.0/24	10.23.0.0/16	Infra specific ports

**Tenant C VNet** 10.24.0.0/16

Availability Zone 1, Availability Zone 2, Availability Zone 3

Source	Destination	Protocol
192.168.230.0/24	10.24.0.0/16	Infra specific ports

**Azure VMware Solution**

Management Segment CIDR: 100.72.x.x/16

Infrastructure Segment CIDR: 100.72.x.x/16

Tenant A Segment CIDR: 172.28.8.0/24

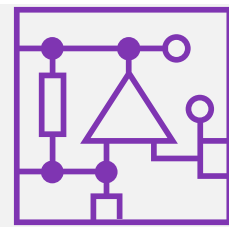
Tenant B Segment CIDR: 172.28.8.0/24

Tenant C Segment CIDR: 192.168.234.0/24

Management Gateway, Compute Gateway, Tier 1 Gateway

Source	Destination	Protocol	Use
55.25.33.21	ExpressRoute	IP	4
ExpressRoute	55.25.33.21	IP	
Public IP	External IP	Internal IP	2
Public 1	10.0.1.200	172.28.8.200	
Public 2	10.0.2.200	172.28.8.200	
Public 3	10.0.3.200	192.168.234.200	
Public 4	10.0.1.2	172.28.8.2	Web





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**  
 IPsec VPN or ExpressRoute between MSP 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, no static route can be configured on Azure VMware Solution 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 Azure VMware Solution Management segment (or at least vCenter and ESXi). Access from Azure VMware Solution vCenter to on-prem infrastructure services (Active Directory, DNS, Content Library, ...)
- 4 Routed 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.
- 5 Firewall rules for Network segments**
  - Allow connectivity between Infra & Management
  - Allow connectivity between Infra & on-prem infrastructure subnet
  - Allow connectivity between workload segment, VNets and on-prem application subnets
- 6 Infrastructure VMs**  
 Deploying infrastructure VMs 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
- 7 DNS Configuration**
  - Tenant workloads should infrastructure DNS or Azure DNS
- 8 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 to tenants
  - Allow access from/to VNet subnets and External Network segments in the Compute Gateway and through IPsec VPN and Firewall Rules.

