Asset Light Provider Model – Tenant and Internet Connectivity

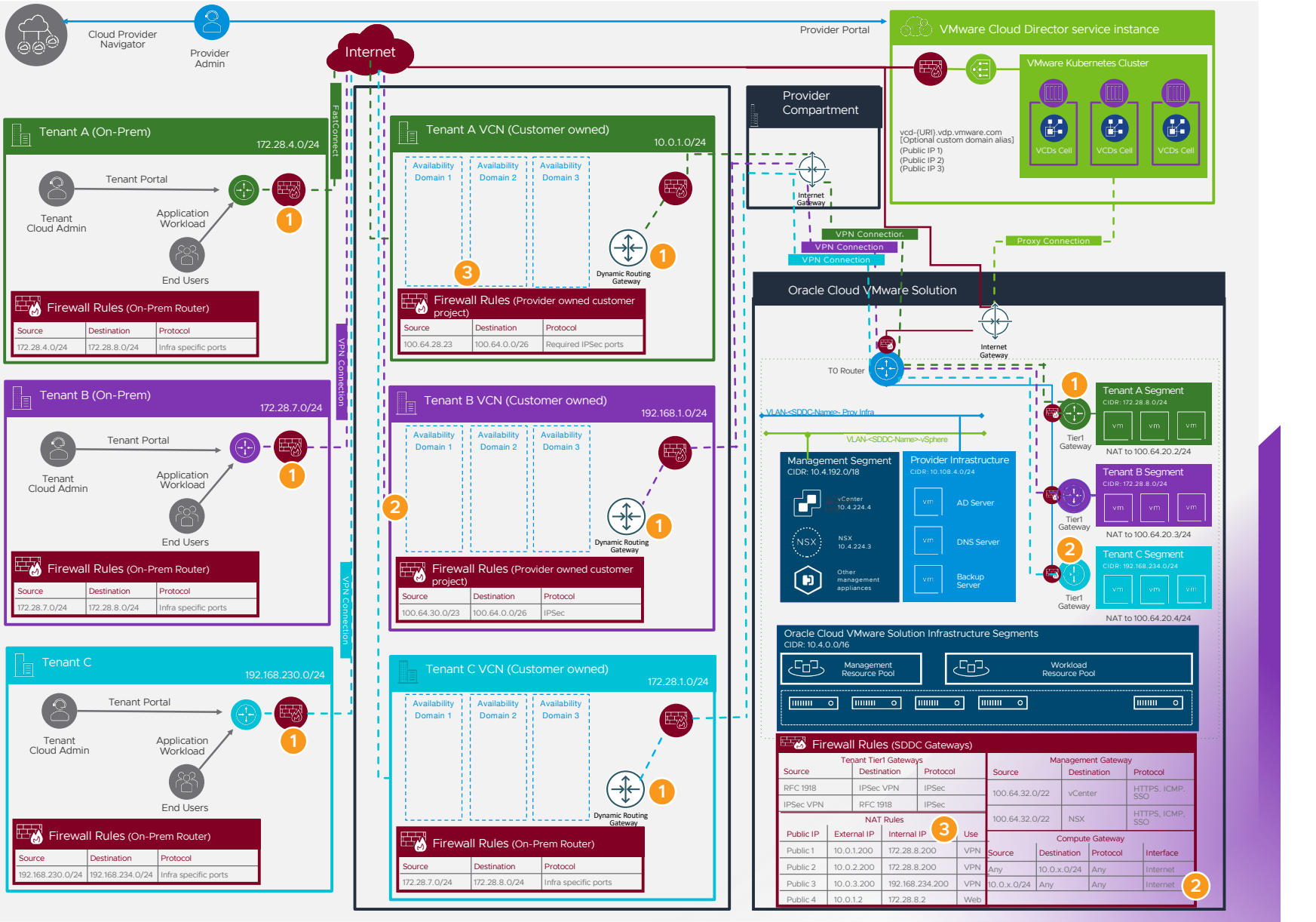
This reference architecture provides generic guidance for an asset light Provider deploying multi-tenant customers in VMware Cloud Director service with Oracle Cloud VMware Solution.

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.

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 Tier 1 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 is the Tier 1 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.
   - Tier1 Gateway firewall rules will govern access to tenant workloads.

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.



Asset Light Provider Model – VPC and Native OCI Connectivity

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 Provider connectivity
IPsec VPN 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 Customer to Provider VCN connectivity (Optional)
This will allow connectivity to the provider VCN from the customer owned VCN.
- If customer VCN to provider VCN connectivity is required, they can leverage local peering via DRG.

3 Service Gateway
This will allow connectivity from the Provider or the customer VCN's to services leveraging OCI Native Services (Object Storage, File Storage, Big Data, Databases, etc.) and traditional Virtual Machines to tenants
- Allow access from/to VCN subnets and External Network segments in the Compute Gateway and through IPsec VPN and Firewall Rules.

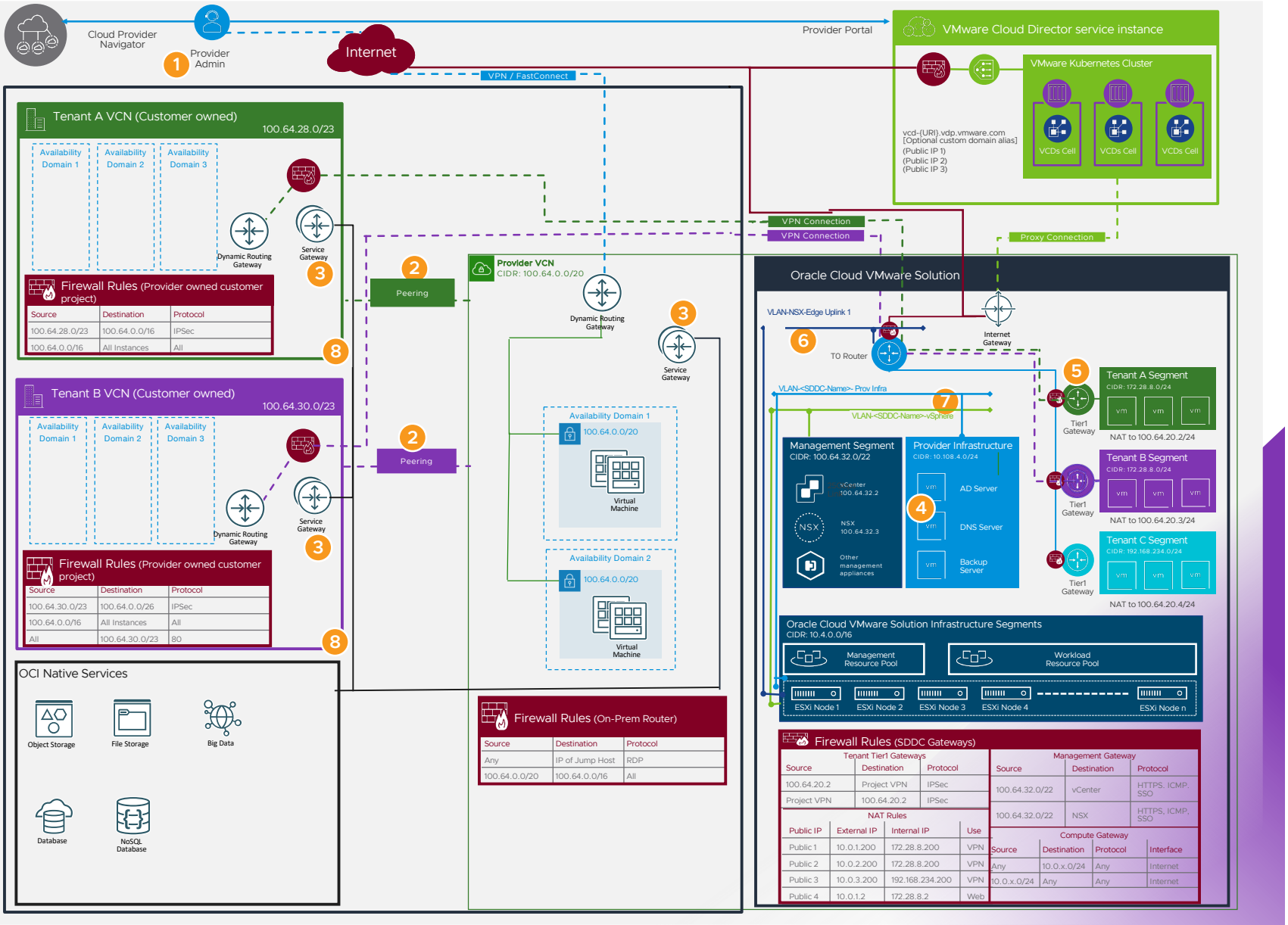
4 Infrastructure VMs
Deploying infrastructure VMs inside OCVS is recommended to provide reliability and performance to application workloads.
Usual infrastructure components are (but not limited):
- Active Directory (RODC might be considered)
- DNS Server
- Backup Server

5 DNS Configuration
- Tenant workloads should use Tier1 Gateway DNS
- Provider can configure Tier1 Gateway DNS forwarder to use custom DNS server

6 VCN Connectivity to OCVS
- Connectivity from OCVS to the provider VCN is direct to the VCN via the Tier 0 NSX edge uplinks.
- Distributed port groups are used to connect

7 vSphere Infra Connectivity
- Connectivity from vSphere infra and provider infra via distributed port groups.

8 Customer Managed
- The customer owned VCN is managed by the customer
- Customer will be required to setup connectivity to/from other VCN's their self with information supplied by provider



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**
IPsec VPN 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.

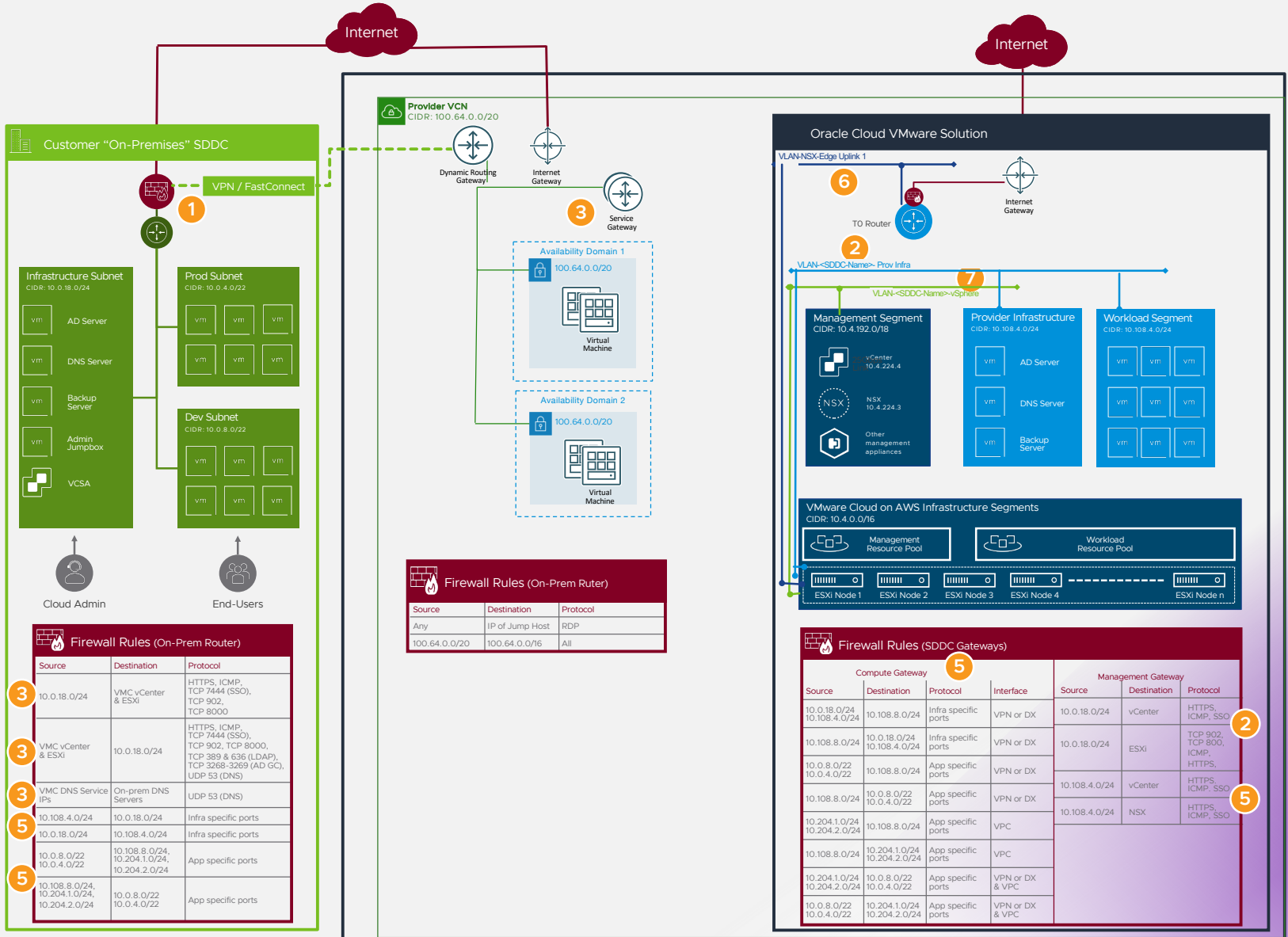
2. **Firewall rules** for vCenter Access.
   - If On-Prem connectivity is configured, allow infrastructure on-prem subnets to access vCenter & ESXi (allowing remote console, vMotion and possibly Hybrid Linked Mode).
   - Otherwise, access can be allowed from public Internet but it is highly recommended to limit it to few trusted public IPs (not detailed here)

3. **On-Prem Firewall**
Access from on-prem subnets to OCVS Management segment (or at least vCenter and ESXi).
Access from OCVS 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, GCP VPC Subnets and on-prem application subnets

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



Firewall Rules (On-Prem Router)

Source	Destination	Protocol
Any	IP of Jump Host	RDP
100.64.0.0/20	100.64.0.0/16	All

Firewall Rules (On-Prem Router)

Source	Destination	Protocol
10.0.18.0/24	VMC vCenter & ESXi	HTTPS, ICMP, TCP 7444 (SSO), TCP 902, TCP 8000
VMC vCenter & ESXi	10.0.18.0/24	HTTPS, ICMP, TCP 7444 (SSO), TCP 902, TCP 8000, TCP 389 & 636 (LDAP), TCP 3268-3269 (AD GC), UDP 53 (DNS)
VMC DNS Service IPs	On-prem DNS Servers	UDP 53 (DNS)
10.108.4.0/24	10.0.18.0/24	Infra specific ports
10.0.18.0/24	10.108.4.0/24	Infra specific ports
10.0.8.0/22 10.0.4.0/22	10.108.8.0/24, 10.204.1.0/24, 10.204.2.0/24	App specific ports
10.108.8.0/24, 10.204.1.0/24, 10.204.2.0/24	10.0.8.0/22 10.0.4.0/22	App specific ports

Firewall Rules (SDDC Gateways)

Compute Gateway

Source	Destination	Protocol	Interface
10.0.18.0/24 10.108.4.0/24	10.108.8.0/24	Infra specific ports	VPN or DX
10.108.8.0/24	10.0.18.0/24 10.108.4.0/24	Infra specific ports	VPN or DX
10.0.8.0/22 10.0.4.0/22	10.108.8.0/24	App specific ports	VPN or DX
10.108.8.0/24	10.0.8.0/22 10.0.4.0/22	App specific ports	VPN or DX
10.204.1.0/24 10.204.2.0/24	10.108.8.0/24	App specific ports	VPC
10.108.8.0/24	10.204.1.0/24 10.204.2.0/24	App specific ports	VPC
10.204.1.0/24 10.204.2.0/24	10.0.8.0/22 10.0.4.0/22	App specific ports	VPN or DX & VPC
10.0.8.0/22 10.0.4.0/22	10.204.1.0/24 10.204.2.0/24	App specific ports	VPN or DX & VPC

Management Gateway

Source	Destination	Protocol
10.0.18.0/24	vCenter	HTTPS, ICMP, SSO
10.0.18.0/24	ESXi	TCP 902, TCP 800, ICMP, HTTPS,
10.108.4.0/24	vCenter	HTTPS, ICMP, SSO
10.108.4.0/24	NSX	HTTPS, ICMP, SSO