Multi-Tenancy with VMware Cloud Director services

On the VMware Cloud Provider Platform

A Natural Partnership

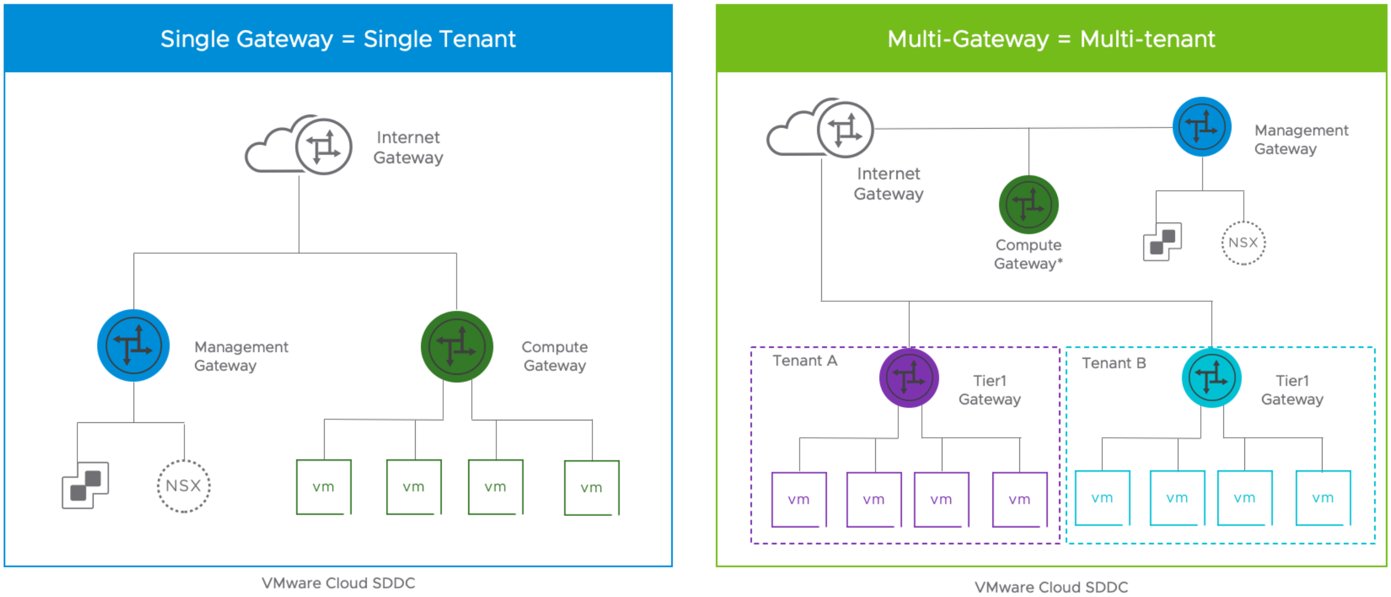
For Cloud and Service Providers

Table of Contents

VMware Cloud Director service on VMware Cloud on AWS SDDC

Cloud Director service's (CDS) Initial Availability provides services to customers on VMware Cloud (VMC) on AWS and leverages Software-Defined Data Center (SDDC) on AWS to provision networking and security services. The primary use cases of VMware Cloud Director service are Asset light geo expansion, Data Center expansion, and Multi-tenancy on VMware Cloud on AWS. The SDDC infrastructure on VMC on AWS consists of vCenter Server, three NSX Manager appliances, and two NSX Edge appliances (Management and Compute Gateways). Using VMware Cloud Director service, the provider can deploy multiple Tier1 gateways in SDDC. This feature allows CDS to reduce the footprint on VMware Cloud on AWS. CDS also empowers its customers to extend self-service cloud services outside their data center while leveraging familiar technologies. FIGURE 1 describes how deploying multiple

Tier1 Gateways allows providers to configure secure, isolated, consistent, and efficient multi-tenant environments using the VMware Cloud Director services.



* Tier1 traffic must be allowed by opening inbound/outbound access in the Compute Gateway

FIGURE 1: Cloud Director Service leveraging Multi-Gateway infrastructure on VMware Cloud SDDC on AWS

VMware Cloud Director Service Architecture and Multi-tenancy

VMware Cloud Director service is a containerized Software as a Service implementation of VMware Cloud Director (VCD). CDS integrates with VMware Cloud on AWS and provides a Cloud Director experience utilizing VMware on AWS infrastructure. To integrate and manage the CDS, the provider can perform the following actions through VMware Cloud Console for CDS instance. The providers can access VCD via Cloud Service Portal and Cloud provider hub.

- Create Instance
- Reset administrator password
- Create Support Bundle
- Associate a VMC SDDC
- Delete Instance

After the association between CDS and SDDC is complete, the provider can view SDDC's vSphere and NSX resources from the VCD provider portal. The customer accesses VMware Cloud Director (VCD) tenant portal to manage tenant applications and services. The customers can also consume API Explorer to perform the same operations using VCD APIs. FIGURE 2 shows the components of SDDC used by the VMware Cloud Director service.

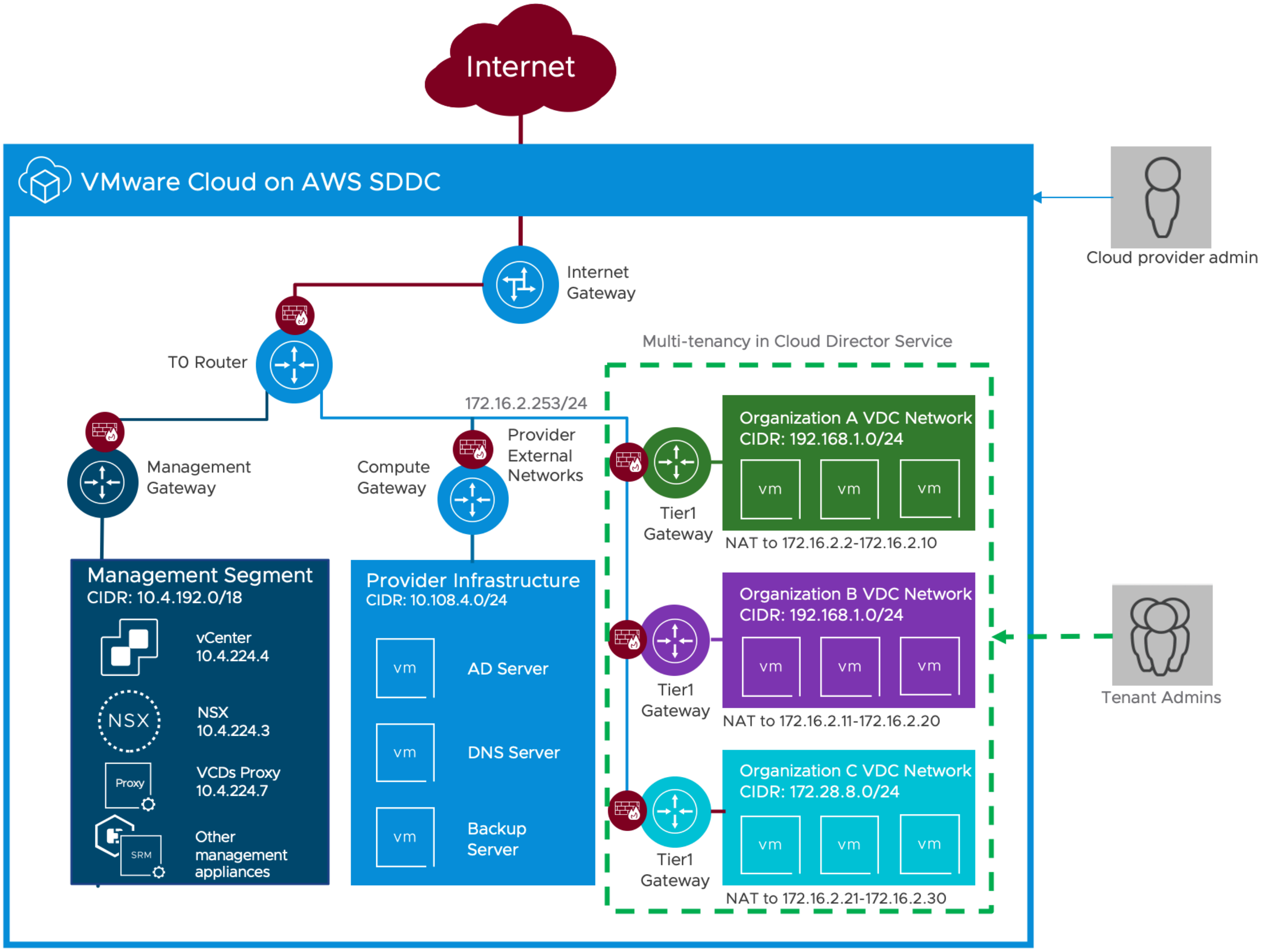


FIGURE 2: VMware Cloud Director services architecture for multi-tenancy on VMware SDDC on AWS

A freshly deployed SDDC on AWS has three gateway types described in the table below. The provider can access these gateways using the Networking and Security tab on SDDC on VMware Cloud console on AWS.

NETWORKS AND GATEWAYS ON VMC ON AWS SDDC	
NETWORKING CONSTRUCT	DESCRIPTION AND FUNCTION
Internet Gateway	• The connectivity to AWS VPC, Internet, or Direct Connect passes through the internet gateway which is backed by an NSX-T Tier-0 Gateway.
Management Gateway (MGW)	• This gateway provides north-south connectivity for the management appliances such as vCenter Server, NSX, HCX, vRealize operations, running in the SDDC.
Compute Gateway (CGW)	• The default compute gateway provides north-south connectivity for the services, which are not tenant workloads, running in the SDDC by the provider.

Management Network	• Management Network is connected to MGW. The management network connects the management appliances using a subset of the CIDR range specified during the SDDC creation.
Compute Network	• Compute Network is connected to CGW. It connects providers workloads and services to support customers in the provider infrastructure. Examples of such services are AD server, DNS Server, Backup Server, and more.

The provider can deploy a new type of gateway called a Tier1 gateway through the Cloud Director provider portal. The Tier1 gateway is a unique edge gateway per customer. When the provider creates an additional edge gateway, each edge gateway creates a separate routing domain and organization network and allows customers to have an isolated and secure environment. FIGURE 2 shows example IP networks where Tenant A and Tenant B use same IP network in the organization VDC network.

VMWARE CLOUD DIRECTOR SERVICE COMPONENTS ON CLOUD DIRECTOR PORTAL	
NETWORKING CONSTRUCT	DESCRIPTION AND FUNCTION
Tier1 Gateway (Edge Gateway)	• Edge gateway that is provisioned per tenant through Cloud Director service by the provider. This gateway provides functions such as firewalls, network address translation (NAT), DNS forwarding, and DHCP service.
External Network	• An External network is a transit network between the Tier-0 router and the Tier1 gateway at the tenant level. • Each edge gateway is assigned one or multiple IP addresses from the external network created in the Cloud Director provider portal.
Organization VDC Network	• This network provides controlled access to machines and networks outside of the VDC via the customer edge gateway. • A tenant can create and manage them via the Networking section in the tenant portal. Each tenant can have one or more networks.

Provider Workflow

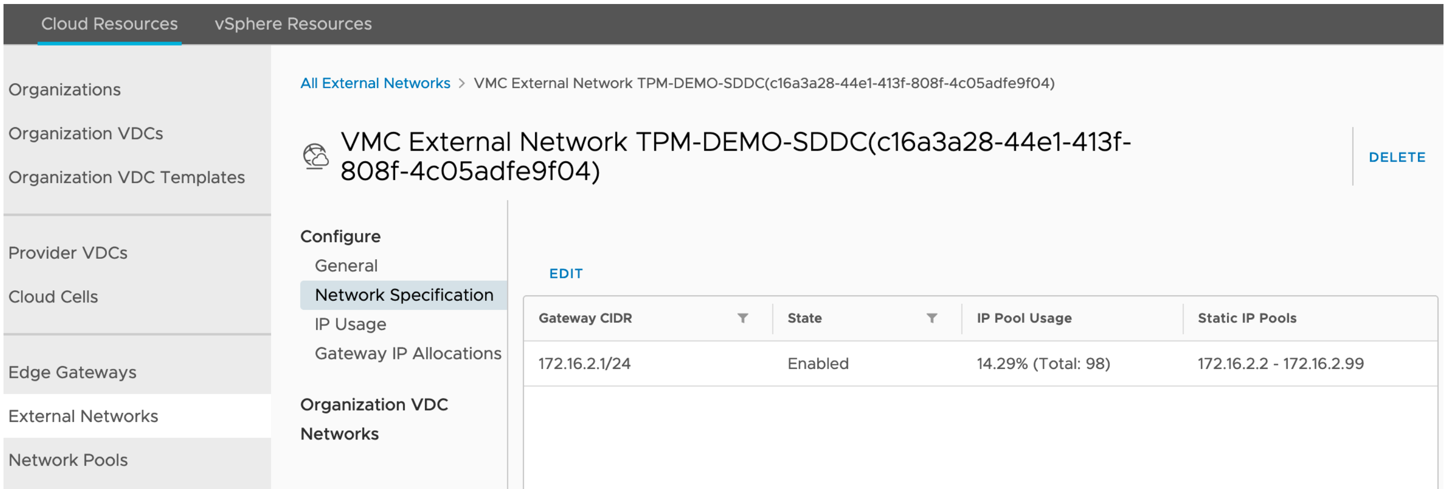
A provider admin must perform some configuration before a customer can get all the benefits from VMware Cloud Director service for VMware Cloud on AWS.

Organization setup is out of the scope of this whitepaper; more information on this aspect of the configuration is available in the VMware Cloud Director Service provider Admin Portal Guide.

To allow a tenant admin to access self-service networking and security services from the tenant portal, the provider must perform the following steps from Cloud Director service provider portal:

Configure the external network

This is a pre-requisite step for creating an edge gateway. An external network is created once the VMware Cloud [GB1]Director service's association is complete with the SDDC on VMC on AWS. The import of external network happens with a subnet from the 169.254.0.0/16 range: this network specification can be deleted and replaced with the network of choice. An Edge gateway must be assigned at least one unique external IP. FIGUREs 3 and 4 show the creation of an External network using the VCD provider portal.

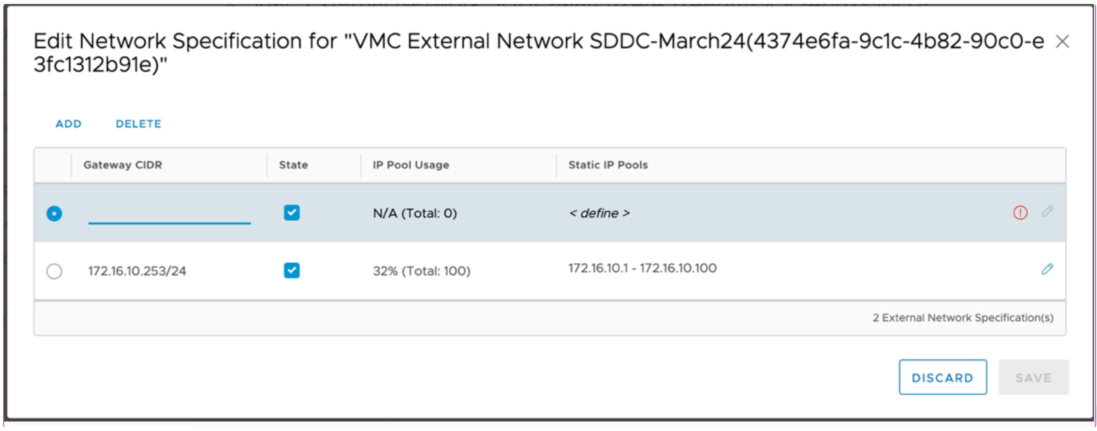


VMC External Network TPM-DEMO-SDDC(c16a3a28-44e1-413f-808f-4c05adfe9f04)

Gateway CIDR	State	IP Pool Usage	Static IP Pools
172.16.2.1/24	Enabled	14.29% (Total: 98)	172.16.2.2 - 172.16.2.99

FIGURE 3: Update External Network range of provider's choice.

The provider admin can also add additional network ranges if required.



Edit Network Specification for "VMC External Network SDDC-March24(4374e6fa-9c1c-4b82-90c0-e3fc1312b91e)"

	Gateway CIDR	State	IP Pool Usage	Static IP Pools
●		☑	N/A (Total: 0)	*< define >*
○	172.16.10.253/24	☑	32% (Total: 100)	172.16.10.1 - 172.16.10.100

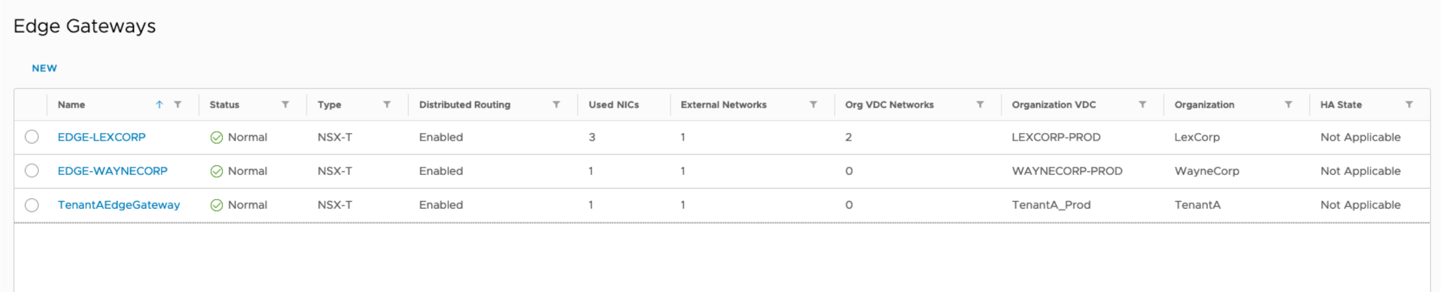
2 External Network Specification(s)

[KL2]

FIGURE 4: Edit or add additional IP network range.

Create an edge gateway

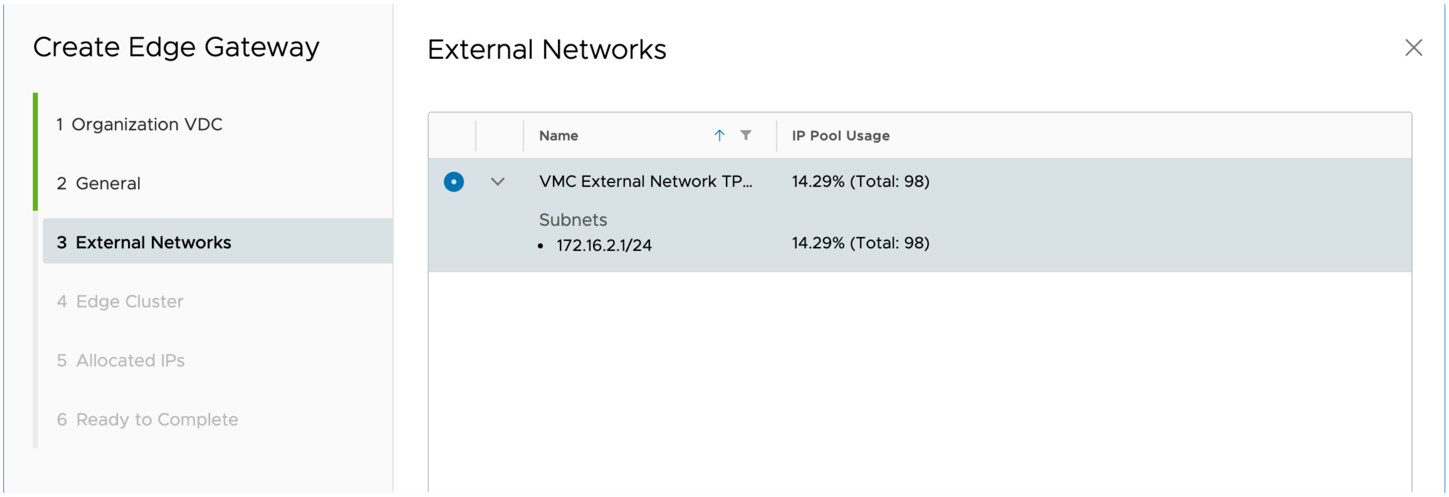
Once the external network is configured, the provider admin can create a unique edge gateway per customer.



	Name	Status	Type	Distributed Routing	Used NICs	External Networks	Org VDC Networks	Organization VDC	Organization	HA State
○	EDGE-LEXCORP	✓ Normal	NSX-T	Enabled	3	1	2	LEXCORP-PROD	LexCorp	Not Applicable
○	EDGE-WAYNECORP	✓ Normal	NSX-T	Enabled	1	1	0	WAYNECORP-PROD	WayneCorp	Not Applicable
○	TenantAEdgeGateway	✓ Normal	NSX-T	Enabled	1	1	0	TenantA_Prod	TenantA	Not Applicable

FIGURE 5: Create a new edge gateway per tenant VDC

After providing a name and the Organization VDC for the edge, the next step is to provide the IP range from the external network's available to which the new edge gateway connects in a VMware Cloud Director service on VMC on AWS.



Create Edge Gateway

1 Organization VDC

2 General

3 External Networks

4 Edge Cluster

5 Allocated IPs

6 Ready to Complete

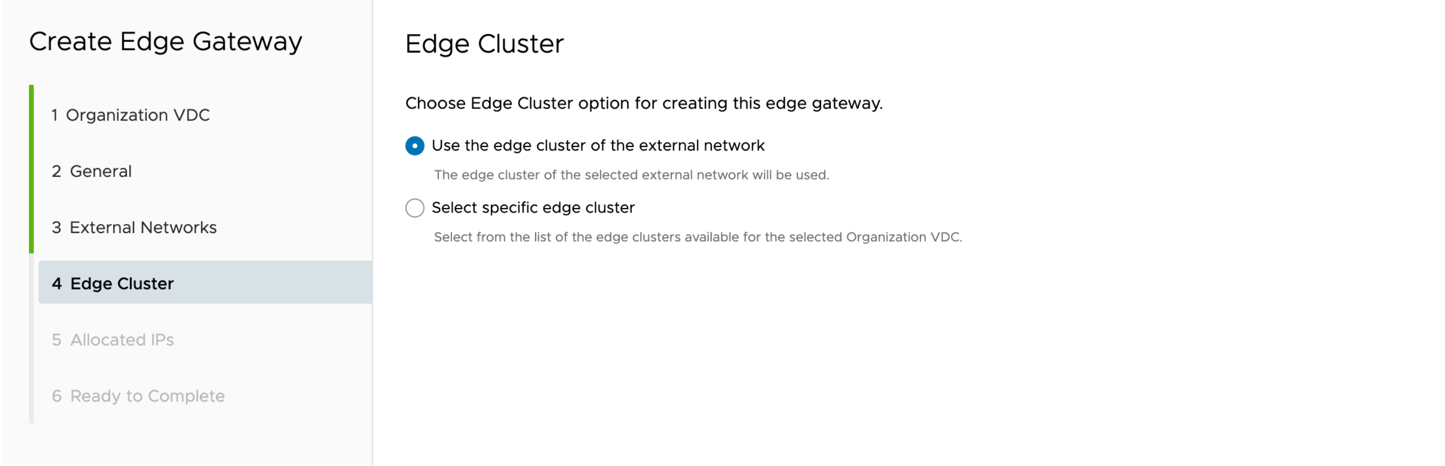
External Networks

		Name	IP Pool Usage
●		VMC External Network TP...	14.29% (Total: 98)
		Subnets • 172.16.2.1/24	14.29% (Total: 98)

[RD3]

FIGURE 6: Create a new Edge gateway and allocate IP range for customer.

An Edge Cluster is a logical construct driving a placement decision of oVDC Edge Gateways. The Edge Cluster is created by the provider administrator and then assigned to Organization VDCs as a primary or secondary instance to the Org VDC Network Profile. In the Edge Cluster [GB4]selection screen, select the "*Use the edge cluster of the external network*" option, and click Next.



Create Edge Gateway

1 Organization VDC

2 General

3 External Networks

4 Edge Cluster

5 Allocated IPs

6 Ready to Complete

Edge Cluster

Choose Edge Cluster option for creating this edge gateway.

● Use the edge cluster of the external network

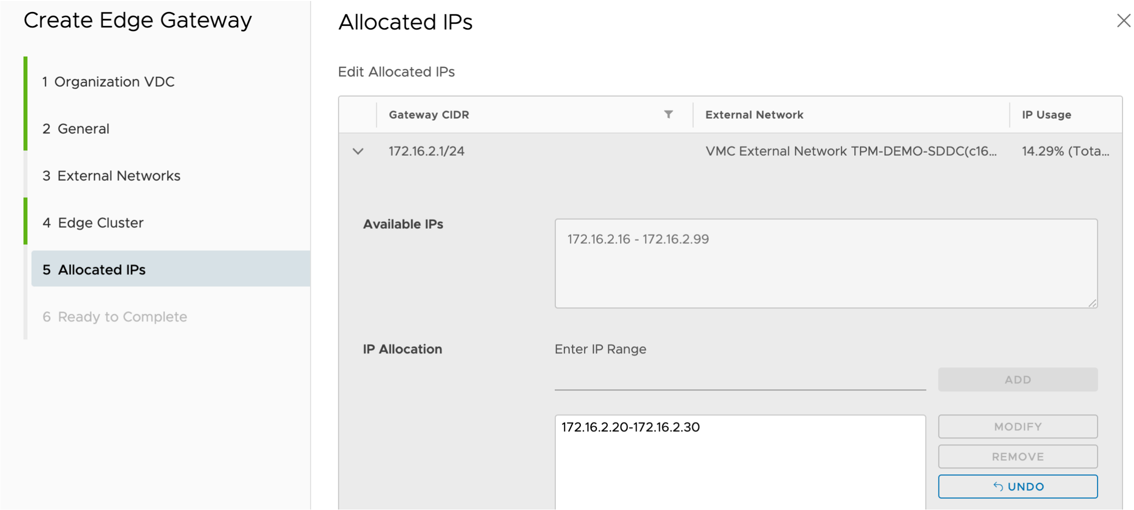
The edge cluster of the selected external network will be used.

○ Select specific edge cluster

Select from the list of the edge clusters available for the selected Organization VDC.

FIGURE 7: Select Edge Cluster of External Network.

The provider admin allocates one or multiple IP addresses of the external network to the edge gateway. When an IP is allocated from the external network to an edge gateway, it is reserved for the edge gateway and removed from the available IPs. This workflow prevents the provider to assign the same IP address or range of IPs to multiple tenants.



Create Edge Gateway

1 Organization VDC
2 General
3 External Networks
4 Edge Cluster
5 Allocated IPs
6 Ready to Complete

Allocated IPs

Edit Allocated IPs

Gateway CIDR	External Network	IP Usage
172.16.2.1/24	VMC External Network TPM-DEMO-SDDC(c16...	14.29% (Tota...

Available IPs: 172.16.2.16 - 172.16.2.99

IP Allocation: Enter IP Range

172.16.2.20-172.16.2.30

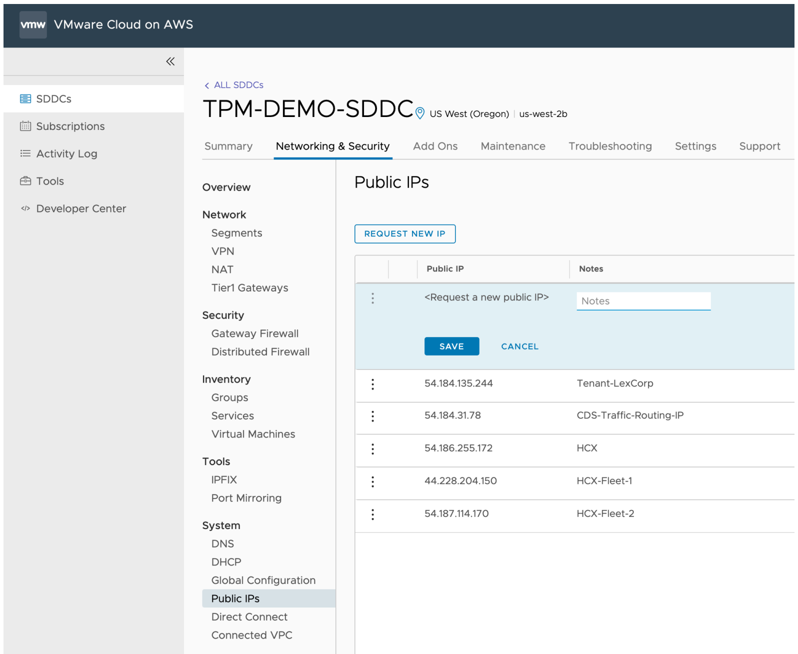
FIGURE 8: Allocate IPs from available External IPs from the IP pool

After configuring the external network, deployment of a new edge gateway and managing services requires identical steps in the multi-tenant environment from the provider VMware Cloud Director portal. Customers can initiate tenant network operations from this point.

Providers can use VMware Cloud console when the tenant requests one or more public IP addresses. A SNAT Public IP is available for all workloads to connect to the internet. However, for inbound access to the workload from the internet a public IP address is required in customer organization,

Request a public IP address from AWS

The provider can request a new IP address with one click from the “*Networking & Security*” section in the SDDC in the VMC console. Customers can request multiple public IP addresses.



TPM-DEMO-SDDC US West (Oregon) | us-west-2b

Public IPs

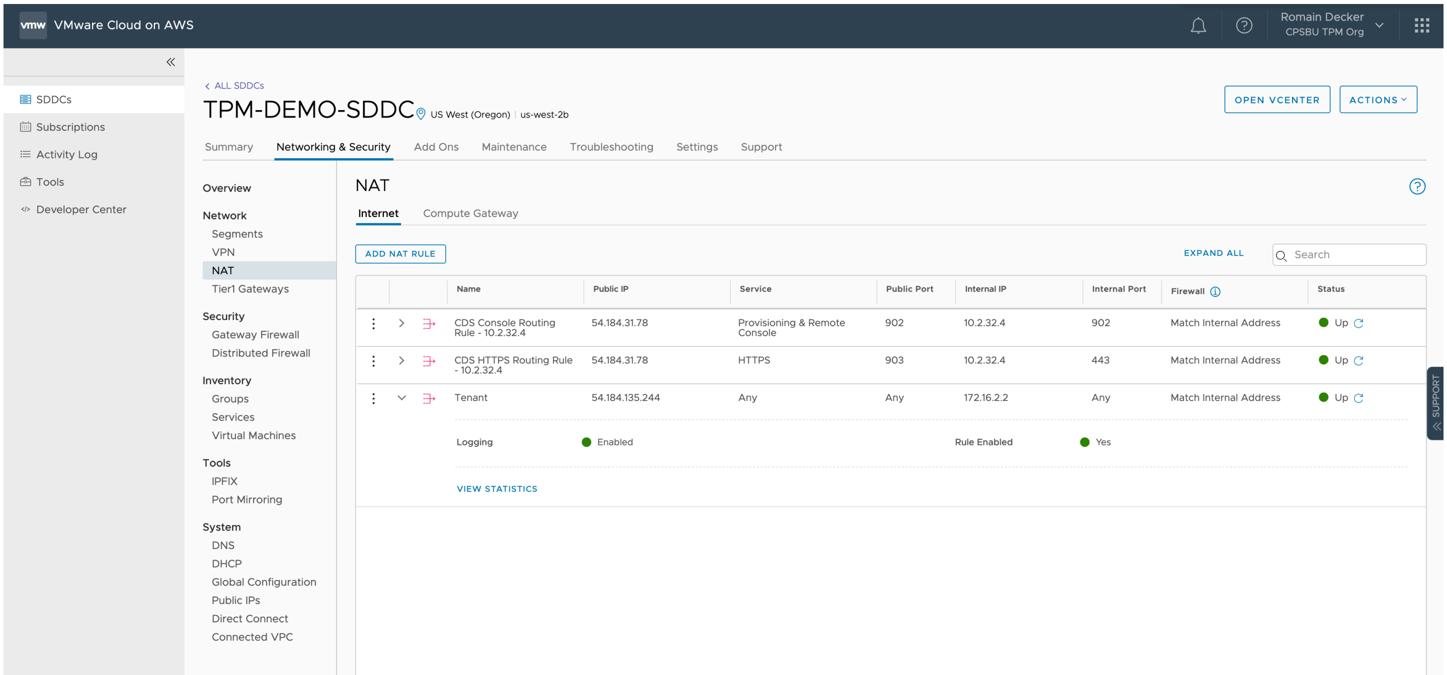
Public IP	Notes
<Request a new public IP>	Notes
54.184.135.244	Tenant-LexCorp
54.184.31.78	CDS-Traffic-Routing-IP
54.186.255.172	HCX
44.228.204.150	HCX-Fleet-1
54.187.114.170	HCX-Fleet-2

FIGURE 9: Request a Public IP address from VMware Cloud console

Create a NAT rule for inbound customer workload access

The provider needs to map the requested public IP address to the customer's external IP to complete the inbound connectivity. The tenant can provide external IP by following two easy steps:

1. Configure an IP address on Virtual Machine with an organization network IP.
2. Create a NAT rule to map the Virtual Machine's IP with an available external network IP, allocated to the tenant. NAT rule creation is covered in the tenant operations section.



Name	Public IP	Service	Public Port	Internal IP	Internal Port	Firewall	Status
CDS Console Routing Rule - 10.2.32.4	54.184.31.78	Provisioning & Remote Console	902	10.2.32.4	902	Match Internal Address	● Up
CDS HTTPS Routing Rule - 10.2.32.4	54.184.31.78	HTTPS	903	10.2.32.4	443	Match Internal Address	● Up
Tenant	54.184.135.244	Any	Any	172.16.2.2	Any	Match Internal Address	● Up

Logging ● Enabled Rule Enabled ● Yes

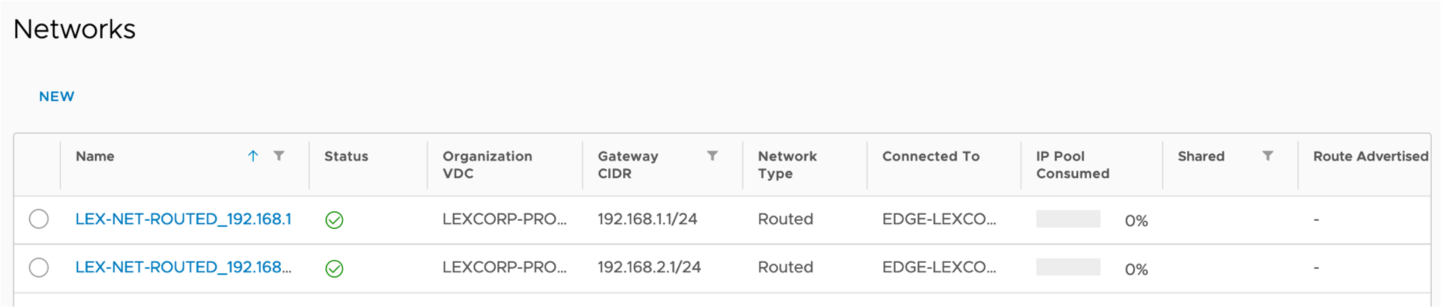
FIGURE 10: Create a 1:1 NAT rule for inbound workload access

Tenant Network and Security Operations

The tenant admin can self-provision network and security services such as Organization VDC network, DHCP service, NAT rules, Edge Firewall, define Static IPs, and more from the CDs tenant portal. Since edge gateway provides the services per customer, multi-tenancy is isolated and secure from a network point of view. provider admin can also perform the tenant operations on behalf of the tenant using the CDs provider portal.

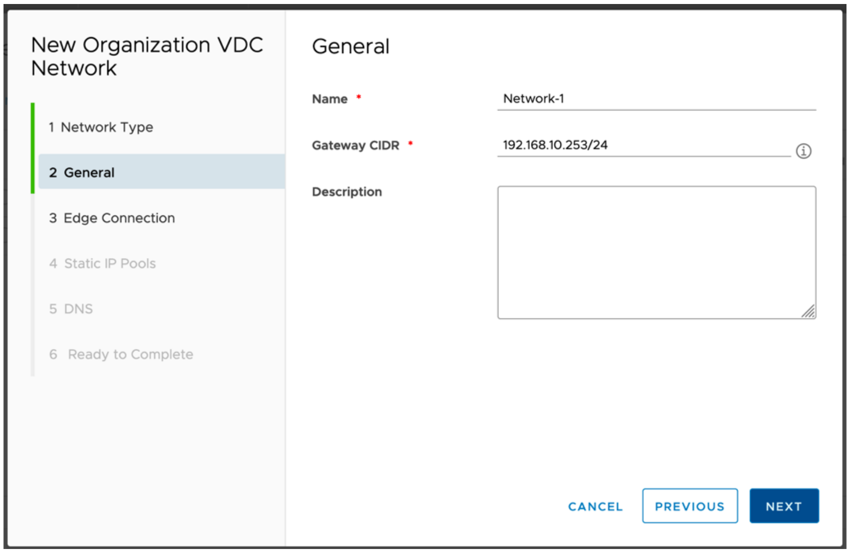
Create an Organization VDC Network

Organization VDC network connects customer workloads in an organization serviced by the Edge gateway. The customers can have more than one organization VDC network. All organization networks are provisioned as routed networks in VMware Cloud Director service Initial Availability.



	Name	Status	Organization VDC	Gateway CIDR	Network Type	Connected To	IP Pool Consumed	Shared	Route Advertised
○	LEX-NET-ROUTED_192.168.1	✓	LEXCORP-PRO...	192.168.1.1/24	Routed	EDGE-LEXCO...	0%		-
○	LEX-NET-ROUTED_192.168...	✓	LEXCORP-PRO...	192.168.2.1/24	Routed	EDGE-LEXCO...	0%		-

FIGURE 11: Create a new Organization VDC network

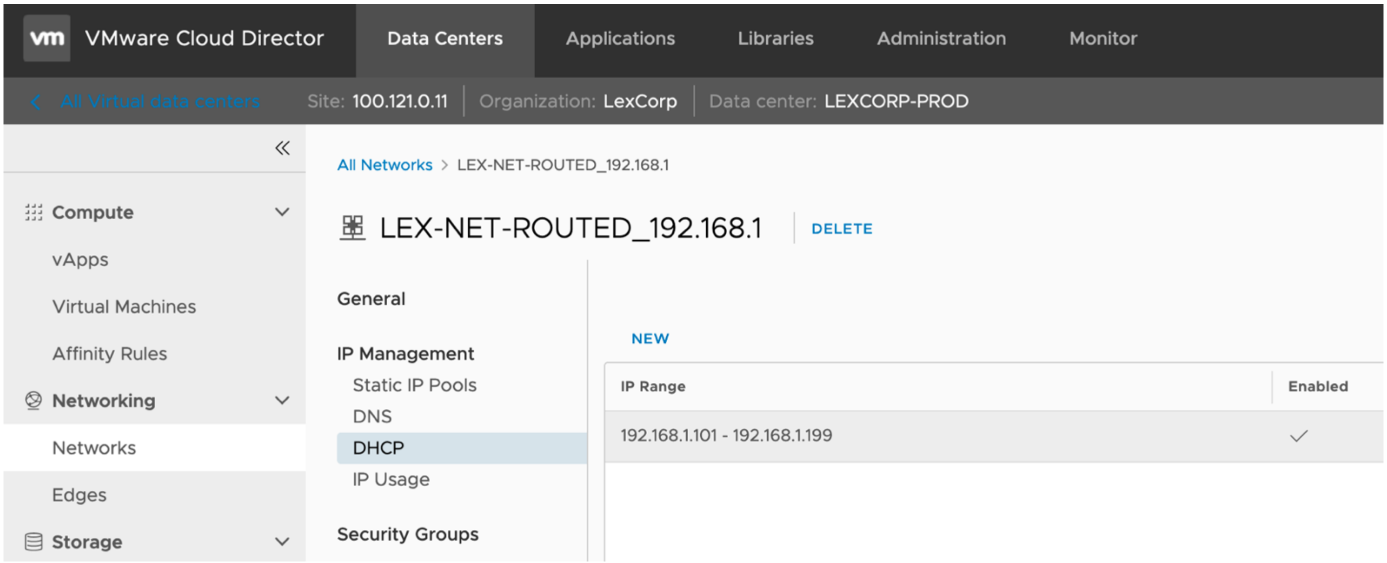


Name *	Network-1
Gateway CIDR *	192.168.10.253/24
Description	

FIGURE 12: Provide Edge selection and gateway CIDR for the network

Configure DHCP Service and DNS forwarder

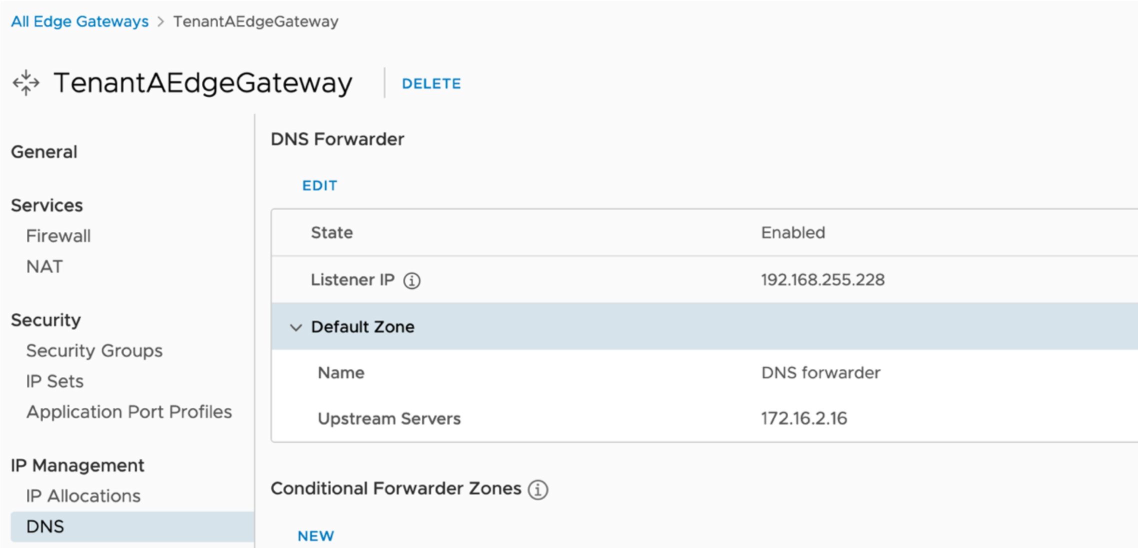
After the organization VDC network is created, the tenant can create a DHCP pool at the organization VDC network level. The edge gateway provides the DHCP service with Static IP Pools and DNS forwarder.



IP Range	Enabled
192.168.1.101 - 192.168.1.199	✓

FIGURE 13: Provision DCHP pool for the workload VMs

The tenant admin can configure DNS forwarding at the edge gateway level. A listener IP is pre-provisioned, which is also an internal IP address from the organization VDC network. DNS forwarding is optional. A tenant can also use any public DNS server IPs in the network settings.



DNS Forwarder

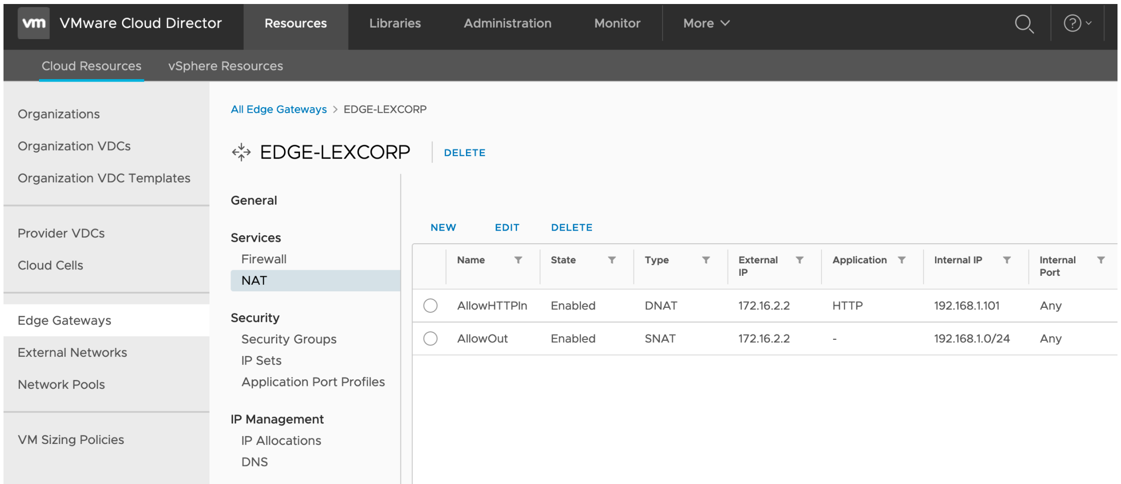
State	Enabled
Listener IP	192.168.255.228
Default Zone	
Name	DNS forwarder
Upstream Servers	172.16.2.16

FIGURE 14: Configure DNS forwarder IP address

NAT Rules

NAT rules perform translation between a customer's allocated external network and Organization network IPs. NAT is the mechanism that permits overlapping IP addresses on in different organization VDC. NAT rules also play an essential role in providing inbound network connectivity. The customer can create SNAT and DNAT rules using the allocated external IPs and internal (Organization VDC) network IPs. While creating the NAT rule, available external network IPs are listed in the information button.

The following NAT rules allow all outbound traffic to the internet (SNAT) by all VMs in network 192.168.1.0/24 and allow web traffic to VM workload with IP address 192.168.20.1 (DNAT).



	Name	State	Type	External IP	Application	Internal IP	Internal Port
○	AllowHTTPIn	Enabled	DNAT	172.16.2.2	HTTP	192.168.1.101	Any
○	AllowOut	Enabled	SNAT	172.16.2.2	-	192.168.1.0/24	Any

FIGURE 15: Example SNAT and DNAT rules to translate incoming HTTP request and all outgoing application requests

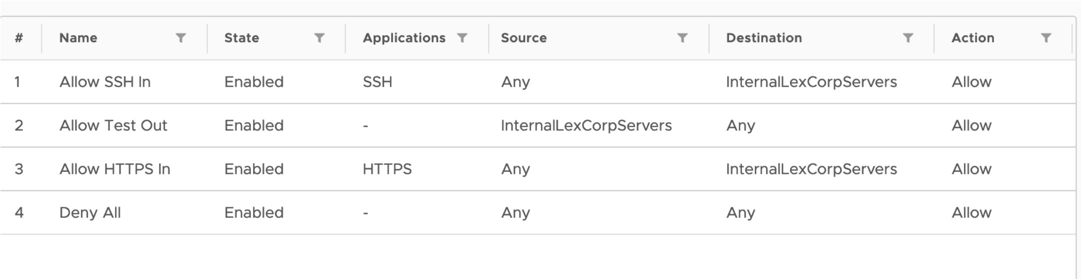
Note: when the DNS forwarder configuration is done on the edge gateway, a corresponding SNAT rule is created to match internal and external network IPs. This rule is service created, so the provider or customer cannot perform delete or create operation.

Edge Firewall Rules

The provider or tenant can manage the edge firewall configuration. The rules are applied to the uplink of the edge gateway, which provides north-south security. The edge firewall allows user to configure rules with the following parameters and options:

- Source, destination: Any or user-created IPset based group (supported input values are IPv4 address, address range, or CIDR).
- Service: Any or specific pre-created provider service. This list contains a service or group of services that providers or tenant admin can use to allow or drop traffic.
- Action: Allow/Deny. The default action is set as Allow.
- State: Enabled/Disabled.
- IP protocol: IPv4 or IPv6 protocol traffic is supported for traffic filtering. The default is set as IPv4.
- Logging: When the Edge rule has logging enabled, and workload traffic matches the Edge rule, a log message is registered.
- Direction: In and Out, In, out.

A sample firewall configuration as follows: The purpose of the following configuration is to allow Web and SSH traffic and block all other applications.



#	Name	State	Applications	Source	Destination	Action
1	Allow SSH In	Enabled	SSH	Any	InternalLexCorpServers	Allow
2	Allow Test Out	Enabled	-	InternalLexCorpServers	Any	Allow
3	Allow HTTPS In	Enabled	HTTPS	Any	InternalLexCorpServers	Allow
4	Deny All	Enabled	-	Any	Any	Allow

FIGURE 16: Example rules for DNS, HTTP, and ICMP Traffics from Workload VM-1

By following the above steps, customers and providers can quickly provide network connectivity using network services to the internet while securing applications using the Edge firewall. The example IP translations from workload VM of a customer to the public IP address is depicted in the diagram below.

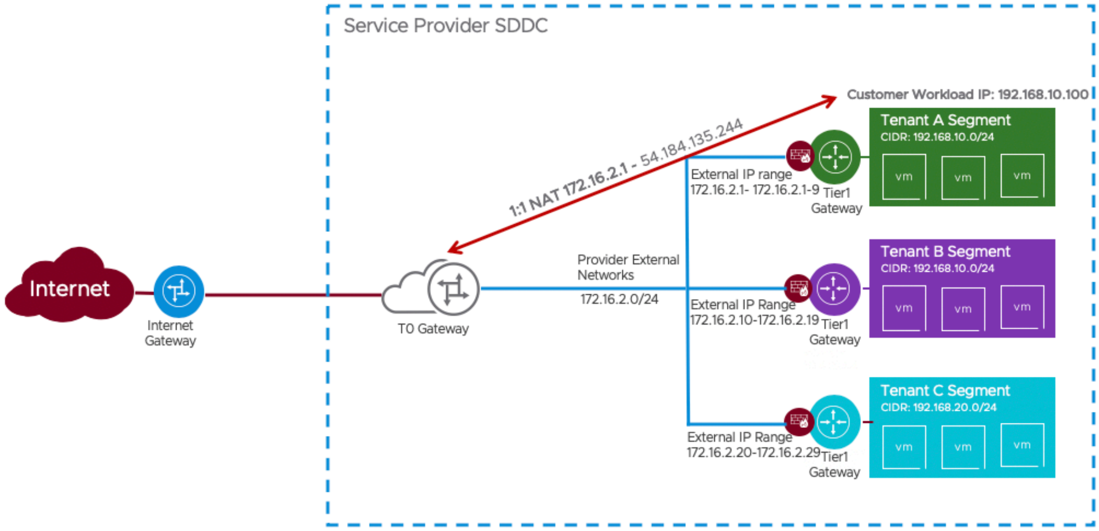


FIGURE 18: IP Translations in VMware Cloud Director service leveraging NAT

Design Considerations for Multi-Tenancy in VMware Cloud Director service

- VPN terminates at the T0 router – Multiple Tier-1 gateways are required in a multi-tenant environment. Hence, the VPN solution provided by NSX cannot be consumed by the tenant. The workaround for this can be to use a non-VMware based VPN solution to provide connectivity.
- Self-service distributed firewall for the tenant – A tenant can consume the edge firewall through the tenant portal and creates rules to filter North-South traffic. However, Distributed firewall (DFW) rules configuration for East-West traffic is not supported[RD5]. As a workaround provider can configure DFW rules in VMware Cloud on AWS.
- Network sharing between multiple organization VDC –Each customer organization VDC is isolated and independent from other customer organizations. The separation is provided by Edge gateway. Network sharing is not possible between the two organizations.
- No vAPP Edge – All tenant edge services are handled by the Tier-1 gateway. vAPP edge services are not supported per vAPP. The vAPP edge services are provided and supported by VMware NSX Edge services. This additional level of Edge services is not supported by NSX-T on VMware Cloud Director™ service.
- AWS native services terminate at Tier-0 – Native AWS services such as Direct Connect, Elastic Network Interface (ENI) terminate at the Tier-0 level of the SDDC.
- The following tables show Maximum supported configurations for SDDC on VMware cloud on AWS and VMware Cloud Director service

VMC ON AWS SDDC LIMITS		
SDDC RESOURCE	PER SDDC LIMIT	TENANT AVERAGE
Tier1 Gateway	16	1
Logical Segments	200	12
CGW Firewall Rules	950	60
CGW NAT Rules	500	30
Public IP Addresses	75	5

CLOUD DIRECTOR SERVICE		
CDS RESOURCE	PER	LIMIT
VCD Org	SDDC	16
VMs	SDDC	2000
VCD Org	VCD Instance	80
VMs	VCD Instance	10000
Concurrent Users	VCD Instance	120
SDDCs	VCD Instance	5

Conclusion

To conclude, we reviewed the networking capabilities for providers and customers for multi-tenancy. We discussed how VMware Cloud Director service introduces consistent, isolated, secure, efficient, multi-tenancy to VMware Cloud on AWS through configuration steps. Cloud Director service also reduces time to provision new virtual data center resources and services. Cloud Director service allows providers to manage Firewall, NAT, Public IP services, and extend the networking and security capabilities to customers. The cloud provider service can genuinely enable the cloud providers to offer services to their smallest or largest size customers while leveraging VMware Cloud on AWS SDDC.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.