



VCF

TechCon

Powered by VMUG

Networking your way in VCF9

- Robin van Altena



VMUGNL
VMware User Group

Robin van Altena

- IT, SDDC, Private Cloud Consultant @*itq*
- vExpert en Broadcom knight



DISCLAIMER



Resources

VMware Cloud Foundation 9 Technical Overview Modernize Infrastructure: Networking

VCF Virtual Networking Technical Reference



By Luca Camarda posted Jun 23, 2025 10:50 AM

This document supersedes the NSX Design Guide starting with VCF version 9.0.

For VCF 5.2 or standalone NSX 4.2 deployments, the content of the NSX Design guide is still relevant.

Download Here

VCF Virtual Networking

VMware NSX is the software component that powers VMware Cloud Foundation's virtual networking capabilities, including Virtual Private Clouds (VPCs) and advanced network services. NSX serves as a foundational component for any private cloud deployment where the goal is to achieve a cloud operational model and provide a true cloud experience for users.

By abstracting network services from underlying hardware and delivering them through software, NSX represents a fundamental shift in how organizations approach network virtualization and security in modern data centers. As enterprises increasingly adopt software-defined infrastructure and cloud-native architectures, NSX provides the critical networking foundation that enables agility, security, and operational efficiency at scale.

<https://community.broadcom.com/blogs/luca-camarda/2025/06/23/vcf-virtual-networking-technical-reference>

VCF 9 Technical Overview | Part 6 | Networking



VMware Cloud Foundation
10.1K subscribers

Subscribe



9



Share



Save



https://www.youtube.com/watch?v=U50t4vKYPCS&list=PL8_k3uUCO39ueFJmiyuNID9UoYIshSsFr&index=8

Recommend

[Resources](#) > [VMware Hands-on Labs](#)

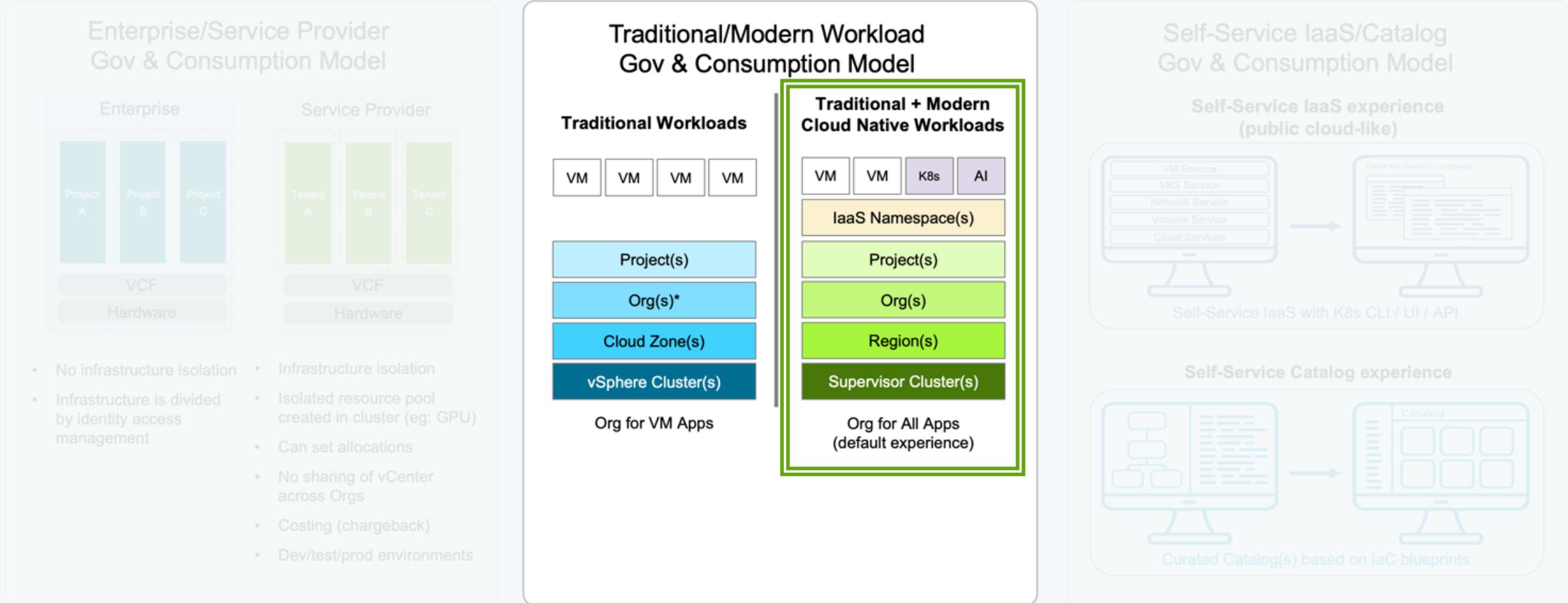
VMware Hands-on Labs

VMware Hands-on Labs provide a quick and easy way to access VMware products and solutions, testing use cases and learning about the latest features with no installation required.

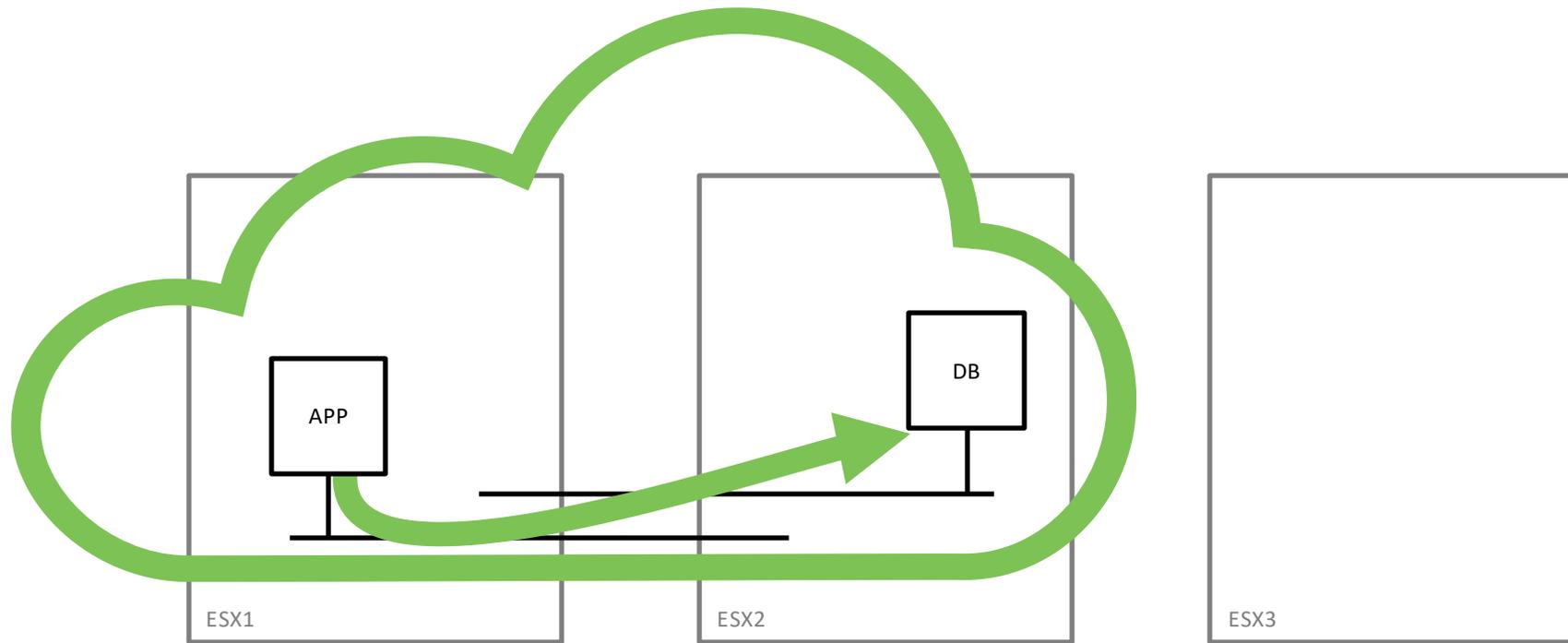
GET STARTED

VCF Automation Governance & Consumption Models

VCF Automation isn't just a simple VM provisioning tool



VCF 9 - Virtual Private Cloud (VPC) Model

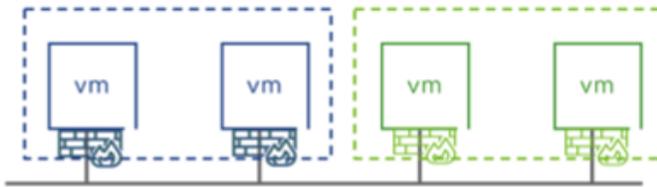


VCF 9 – VPC Model

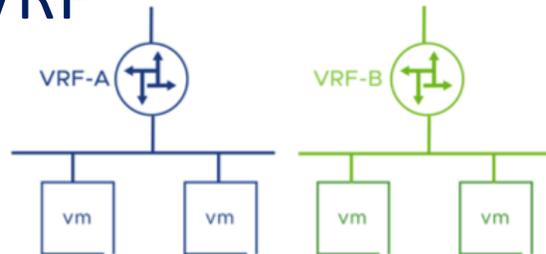
- Public cloud als model
- RABC en Tenant scheiding
- Simpel

VCP en Multi Tenant niet nieuw

- Distributed Firewall

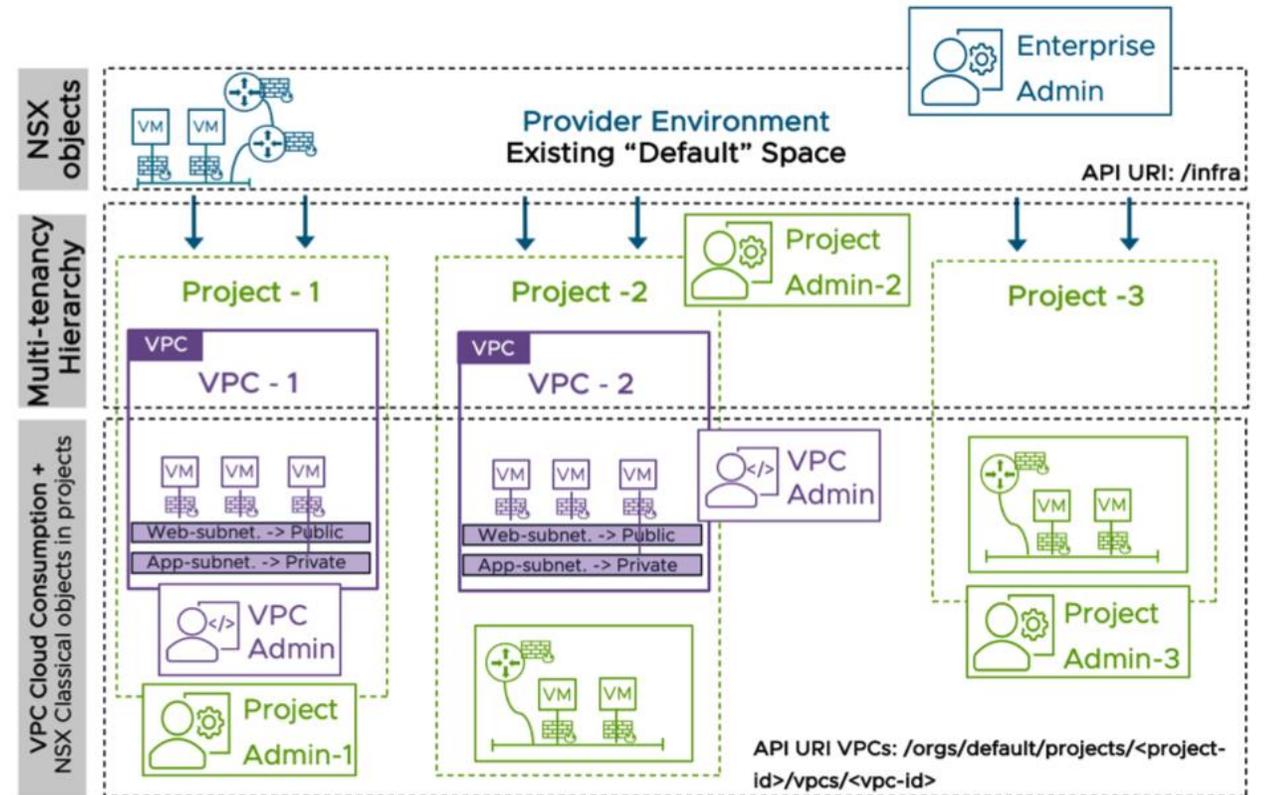


- VRF



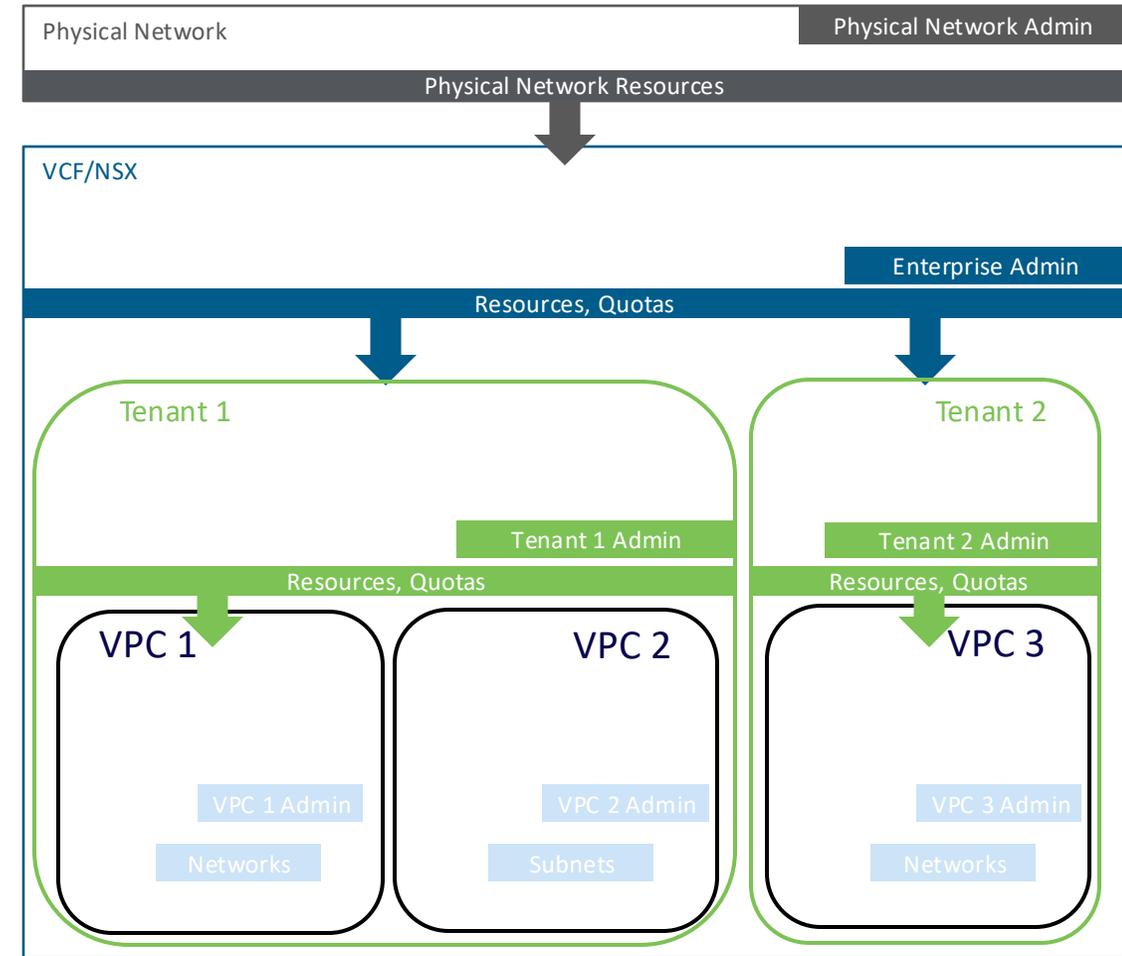
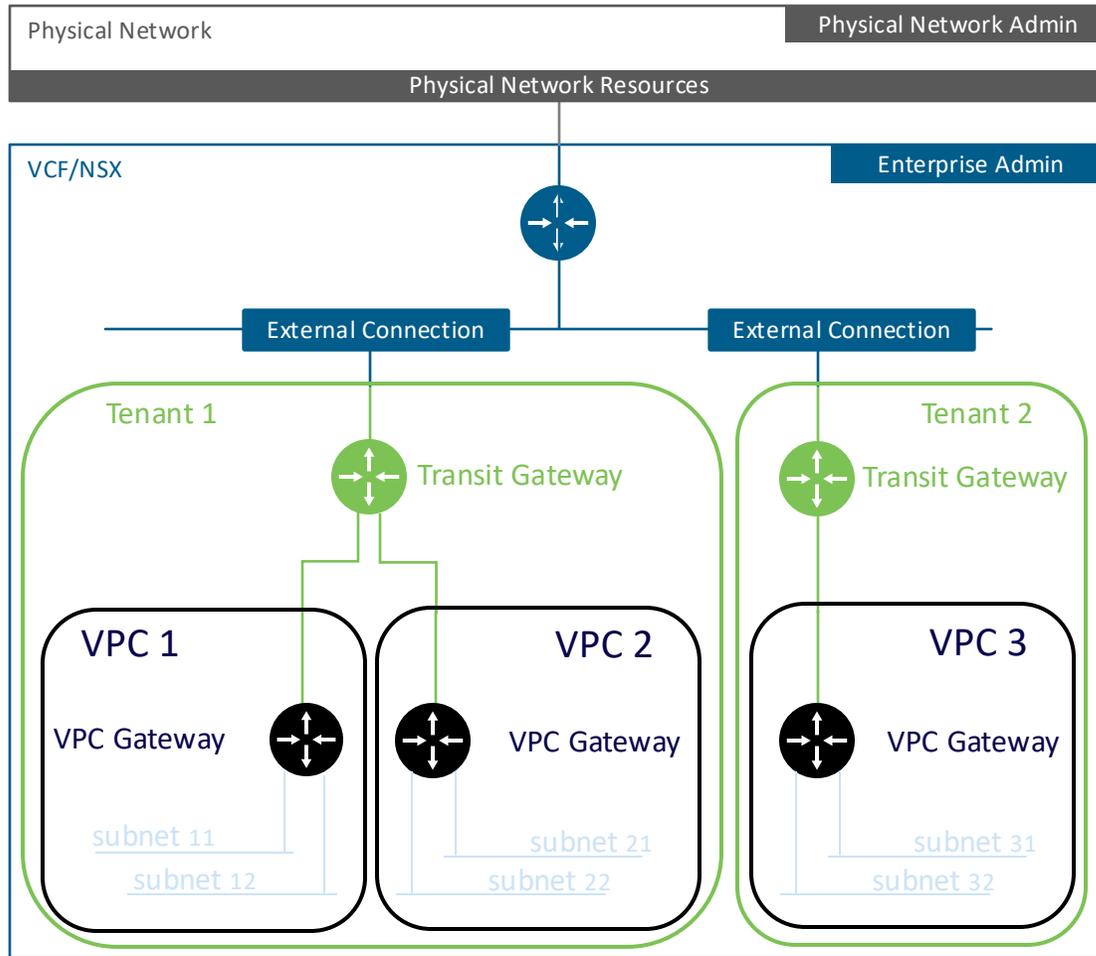
- NSX 4.1.1

- Projects
- VPC

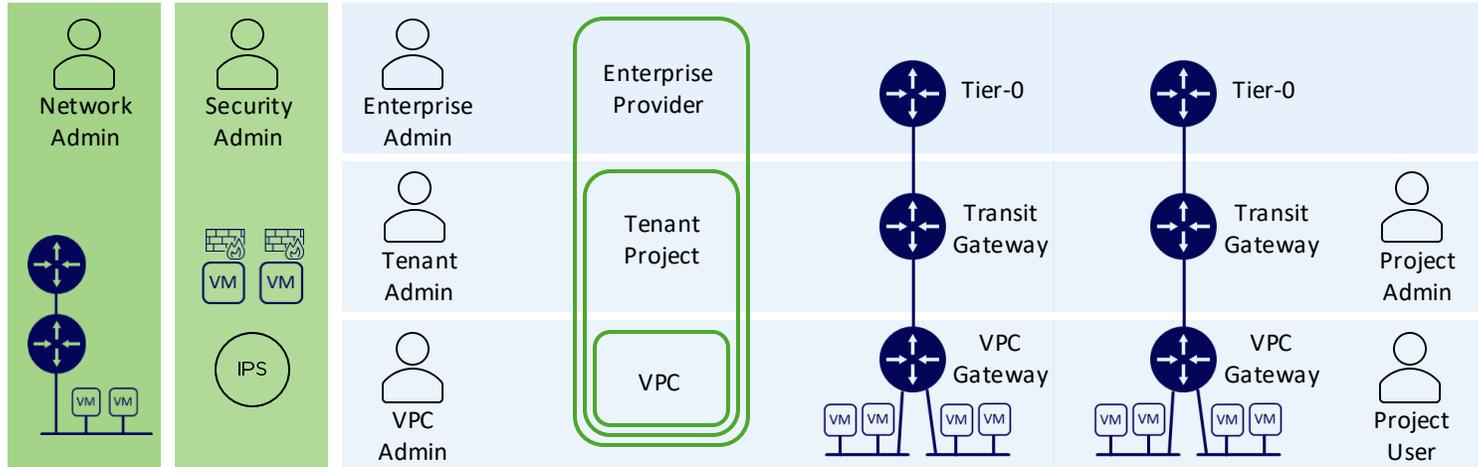


Introduction

Virtual Private Cloud (VPC)

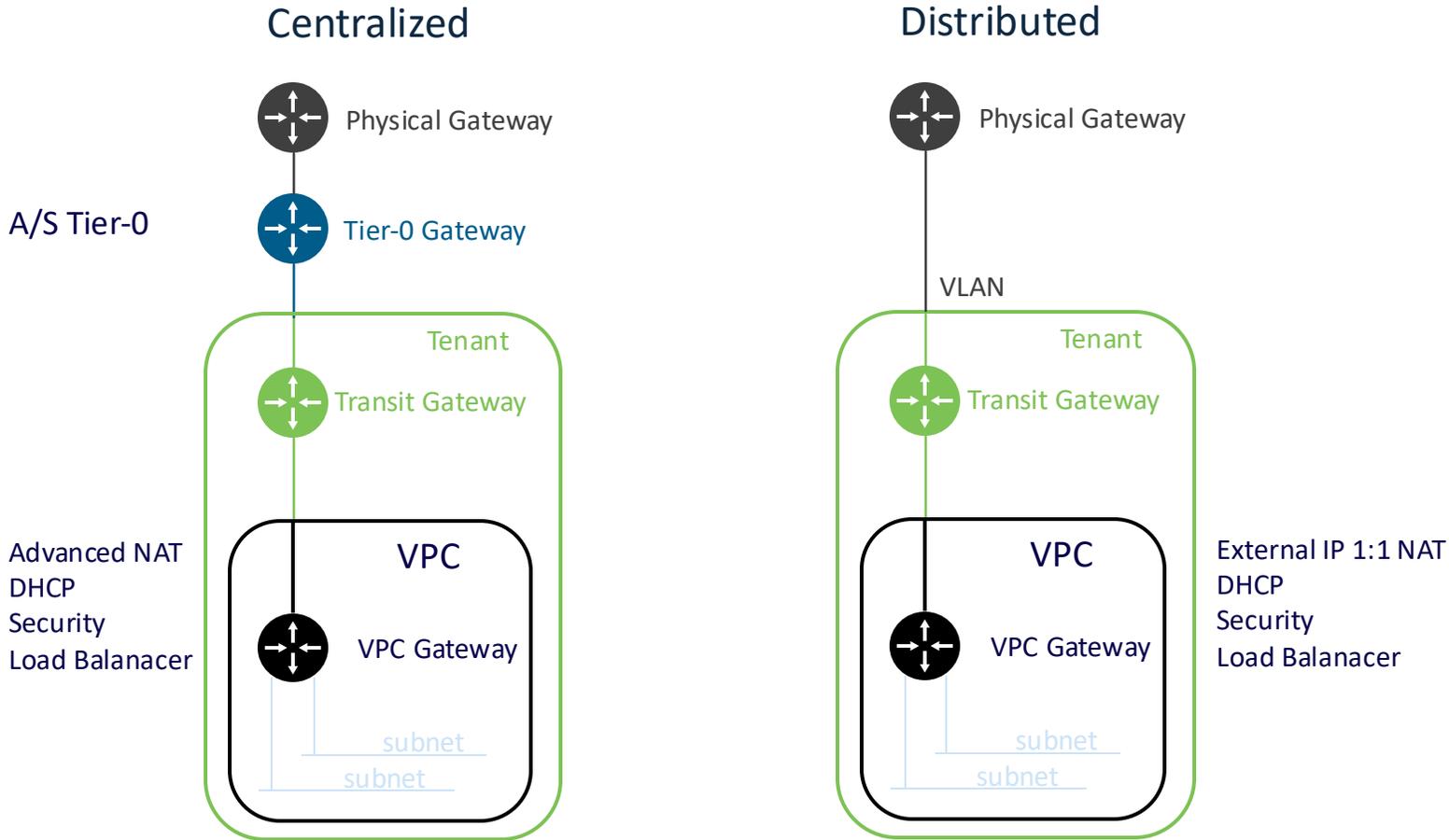


NSX en VCF Roles



User or Role	Responsibilities	Tools and interfaces
Enterprise/Provider/Cloud admin	<ul style="list-style-type: none"> • VCF bring-up • VCF Lifecycle-management • Create Provider Gateway (Tier-0) • Define Tenants and assign resources 	<ul style="list-style-type: none"> • VCF Operations • VCF Automation • vCenter and NSX UI/API
Tenant/Project admin	<ul style="list-style-type: none"> • Create VCF Automation constructs (Project, Namespaces) • Configure Transit Gateway • Create NSX VPC 	<ul style="list-style-type: none"> • VCF Automation • vCenter and NSX UI/API
VPC Admin/Project User	<ul style="list-style-type: none"> • Deploy Workloads and Services • Create VPC objects (Subnets, Firewall rules, Load-balancers, NAT) 	<ul style="list-style-type: none"> • VCF Automation • vCenter and NSX UI/API
Network Admin	<ul style="list-style-type: none"> • Create Provider Gateway (Tier-0) • Create IP-allocations • Create logical Network topologies 	<ul style="list-style-type: none"> • NSX UI/API
Security Admin	<ul style="list-style-type: none"> • Manage Gateways and Distributed firewall policies • Manage tagging and grouping • Manage IDS rules 	<ul style="list-style-type: none"> • NSX UI/API

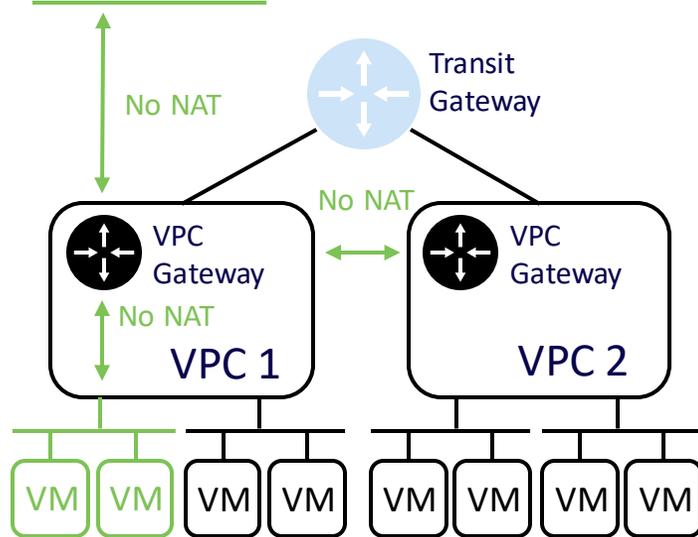
External connectivity Types



VPC Subnets

Public Subnet

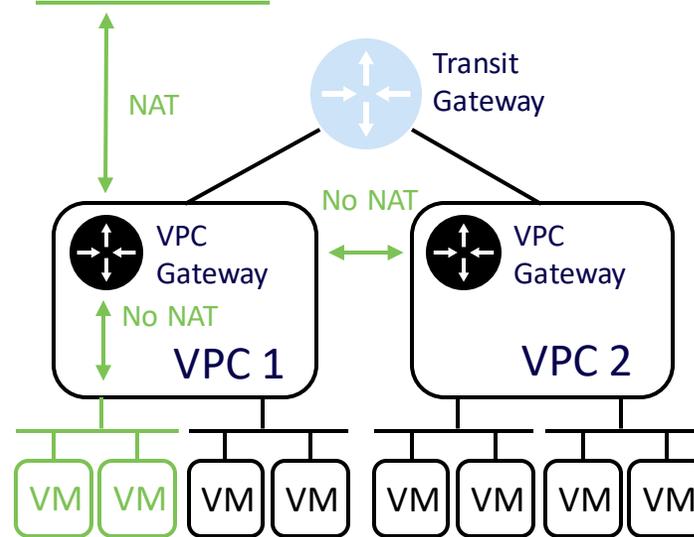
External IP Block



Within VPC No NAT
 Across VPC No NAT
 External (N/S) No NAT

Private Transit Gateway Subnet

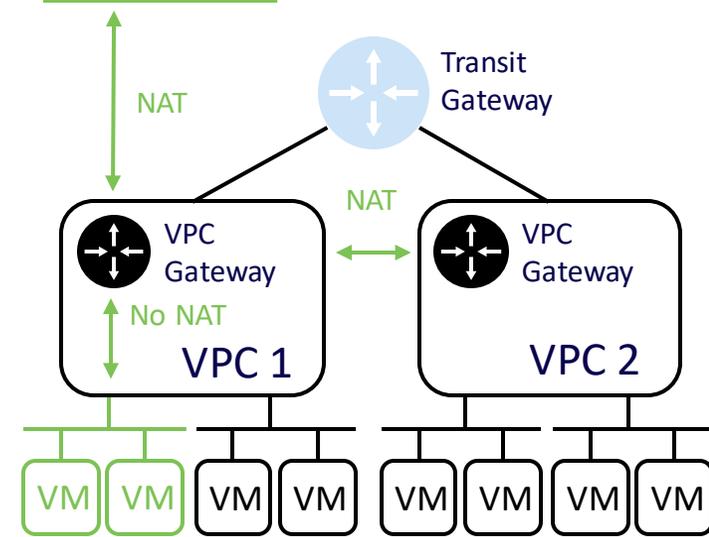
NAT



Within VPC No NAT
 Across VPC No NAT
 External (N/S) NAT

Private VPC Subnet

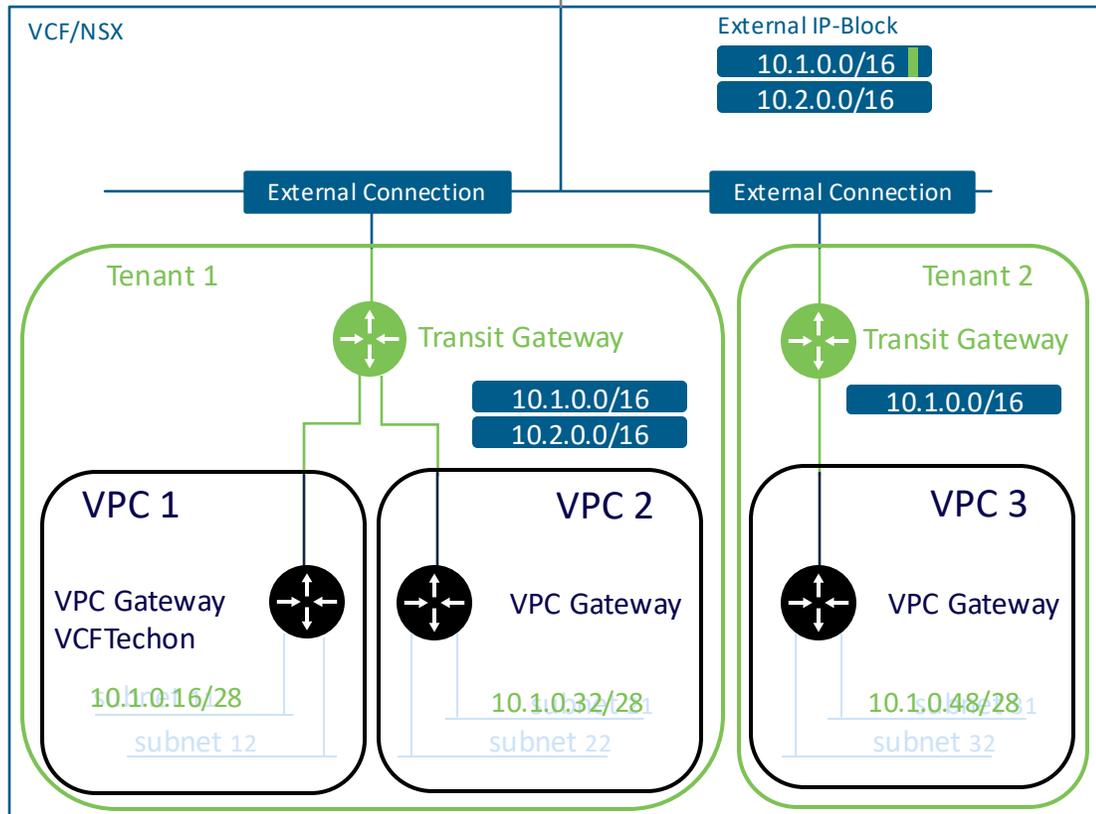
NAT



Within VPC No NAT
 Across VPC NAT
 External (N/S) NAT

VPC - Public Subnet

Physical Network	10.1.0.0/16	Physical Network Admin
	10.2.0.0/16	
Physical Network Resources		



And Quota's

Add Subnet | VCF Techcon

1 Basic Information

2 Ready to Complete

Basic Information

Name *

Access Mode

Auto allocate Subnet CIDR from IP Blocks Yes

Subnet size

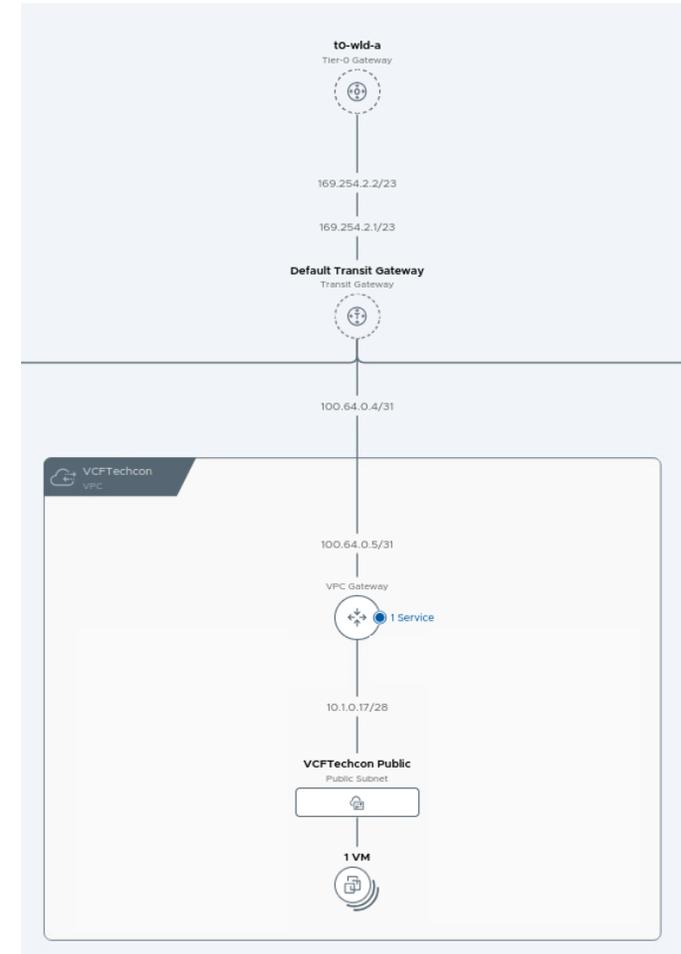
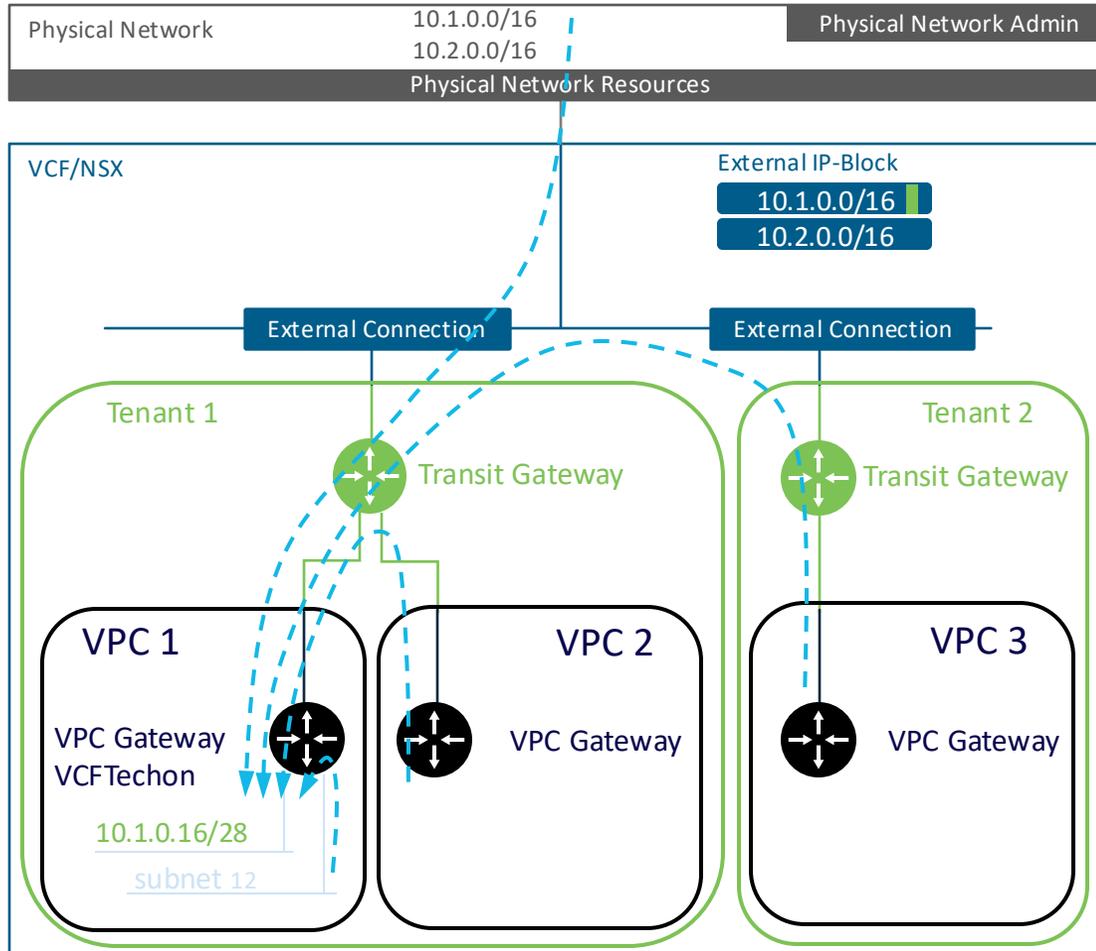
Advanced Settings

Gateway Connectivity Yes

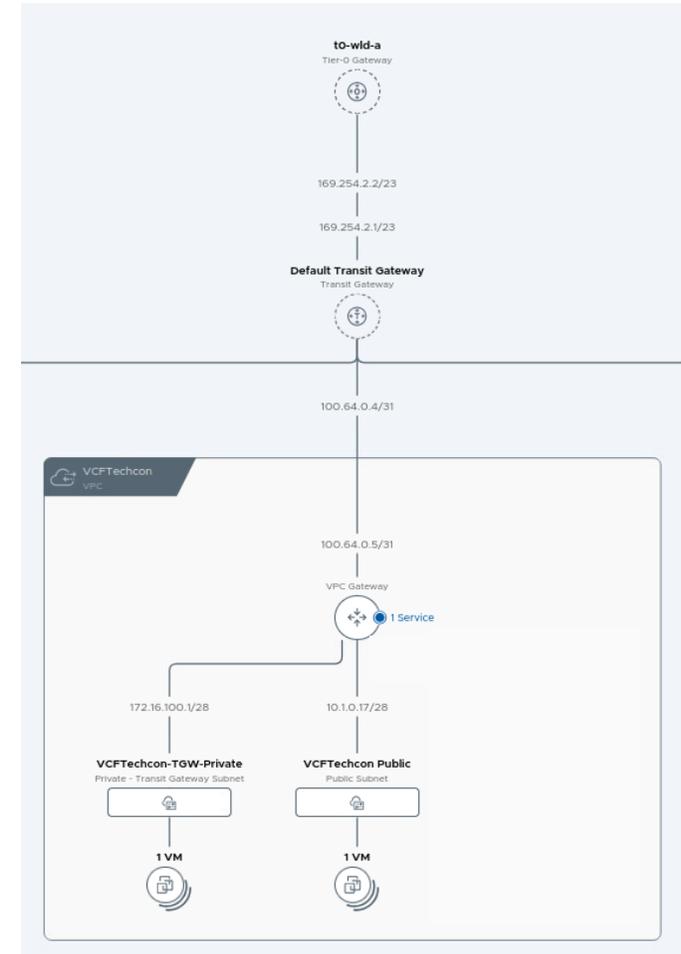
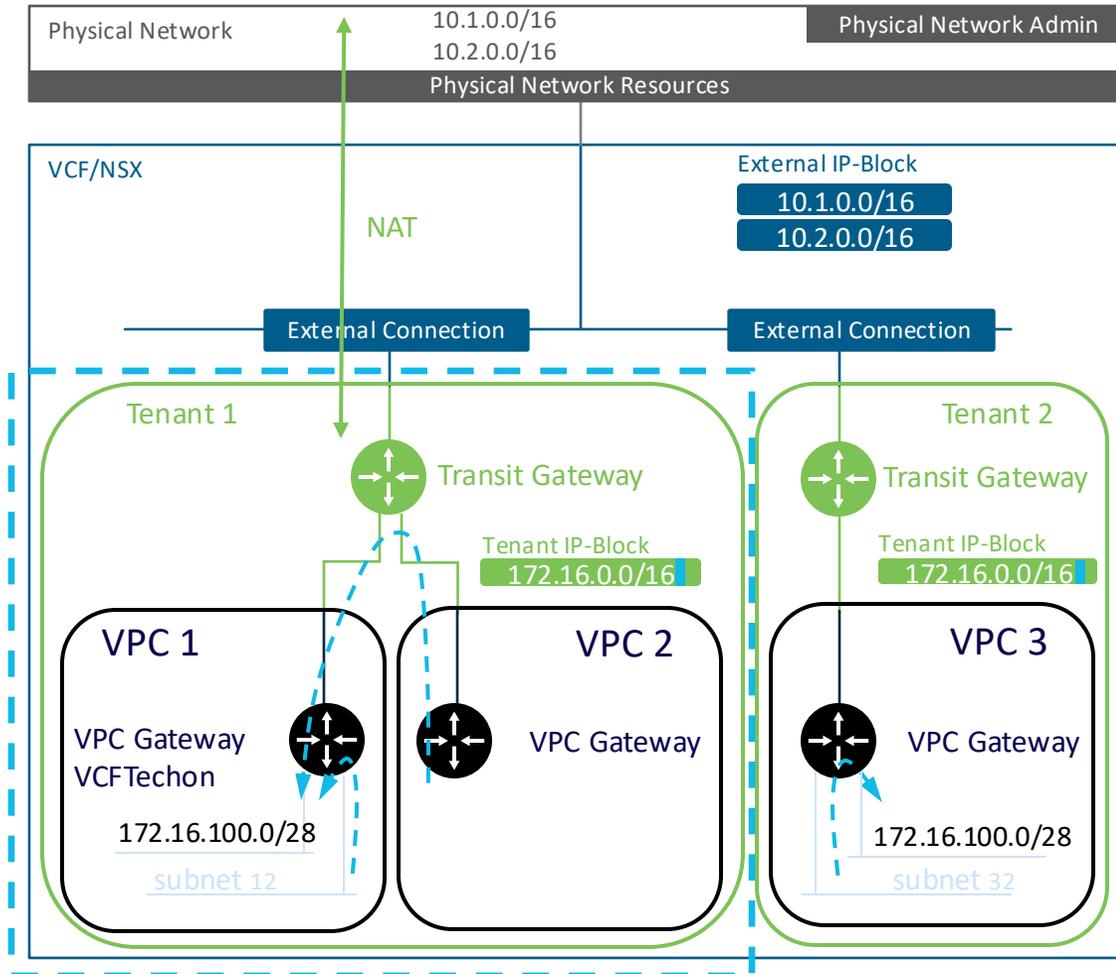
DHCP Config None
 DHCP Server
 DHCP Relay

CANCEL NEXT

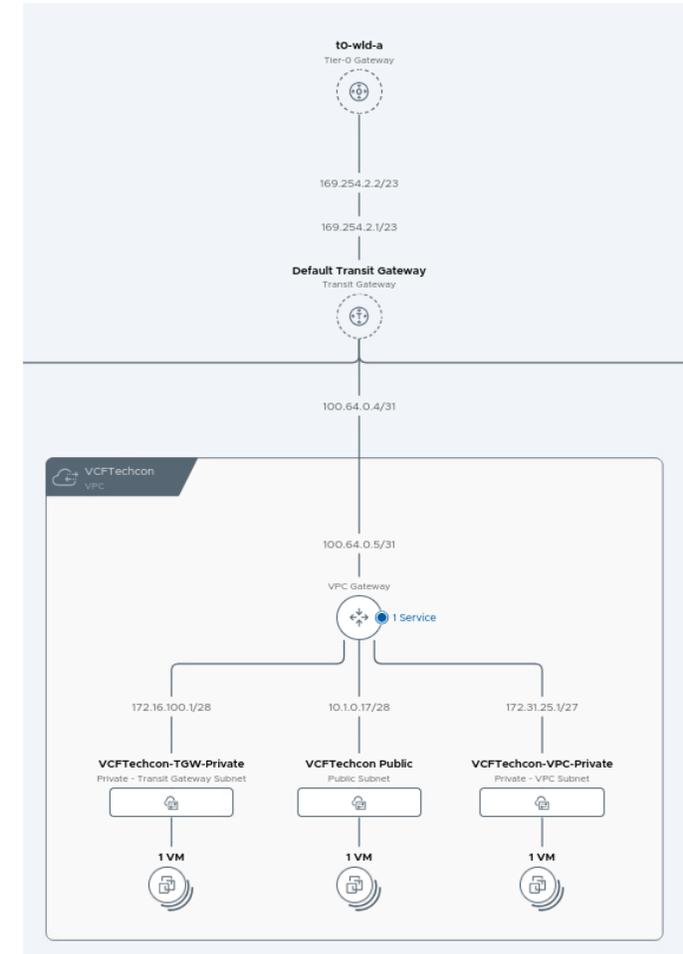
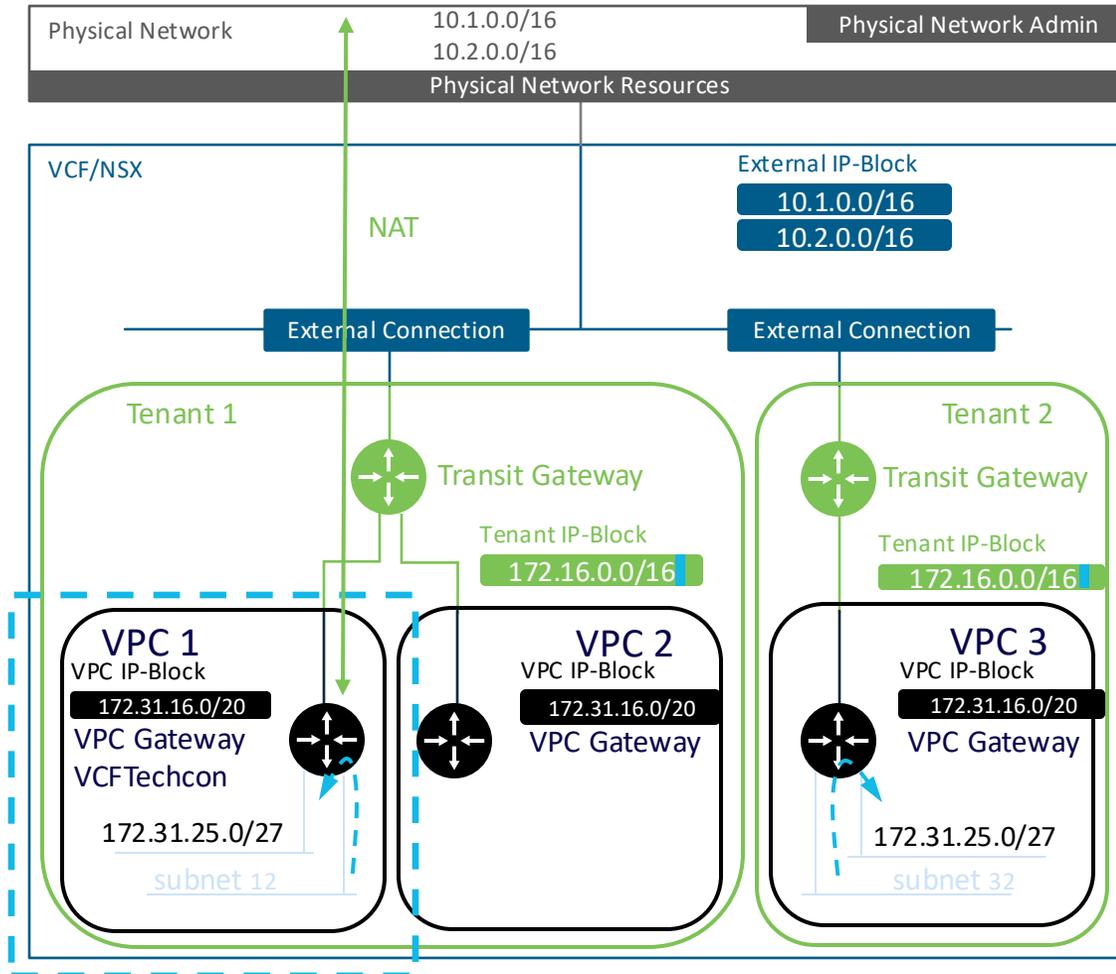
VPC - Public Subnet



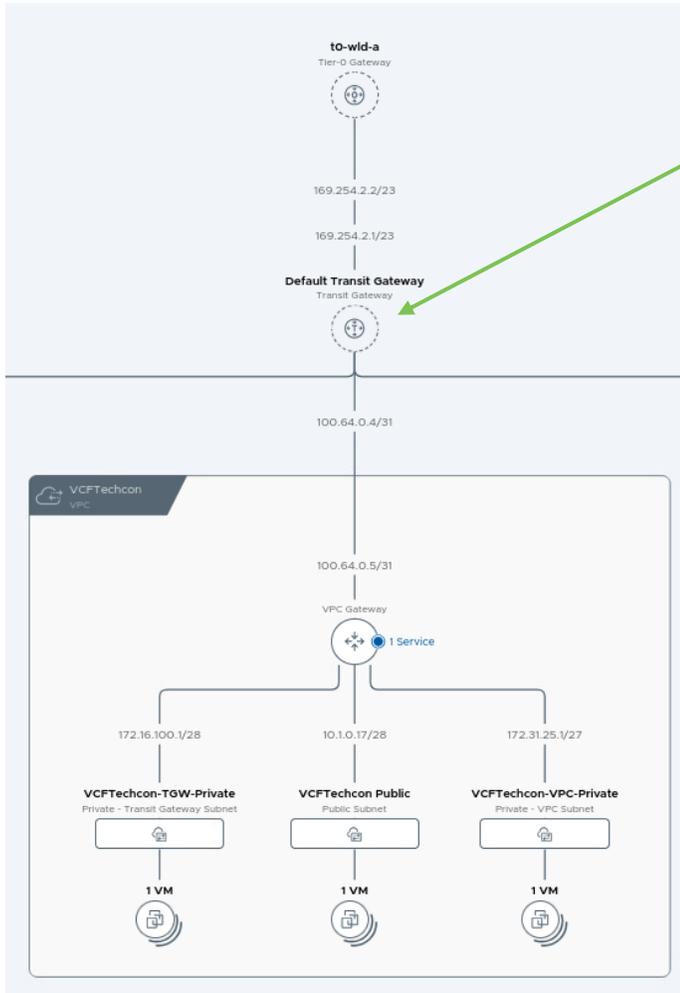
VPC – Transit Gateway Private Subnet



VPC – VPC Private Subnet



TGW routing



```
edge-wld01-01a> get gateways
Thu Oct 23 2025 UTC 18:05:21.511
Gateway
UUID                               VRF    Gateway-ID  Name                                     Type
3c36d4a2-32d9-41b0-b85d-2467ae5c7bc8  0      11          SR-t1-wld-a                             SERVIC
ce88b569-5aaa-42ae-a73b-4edbc5283743  1      13          SR-VRF-Default Transit Gateway          VRF_SE
f251a955-0046-4ea0-bc57-1349553de6c7  2      14          SR-kube-system_99f10881-6962-452     SERVIC
5-9353-c38c22a04726
767428fe-1854-4a7e-a341-36b6305f0057  3      16          SR-vmware-system-supervisor-serv     SERVIC
ices-vpc_edfba51d-1574-4346-bf03
```

```
edge-wld01-01a> vrf 1
edge-wld01-01a(tier0_vrf_sr[1])> get route static
Thu Oct 23 2025 UTC 18:13:37.550

Flags: t0c - Tier0-Connected, t0s - Tier0-Static, b - BGP, o - OSPF
t0n - Tier0-NAT, t1s - Tier1-Static, t1c - Tier1-Connected,
t1n: Tier1-NAT, t1l: Tier1-LB VIP, t1ls: Tier1-LB SNAT,
t1d: Tier1-DNS FORWARDER, t1ipsec: Tier1-IPSec, isr: Inter-SR, isrs: Inter-SR-static
ivs: Inter-VRF-Static, tgws: Transit-Gateway-Static, > - selected route, * - FIB route
```

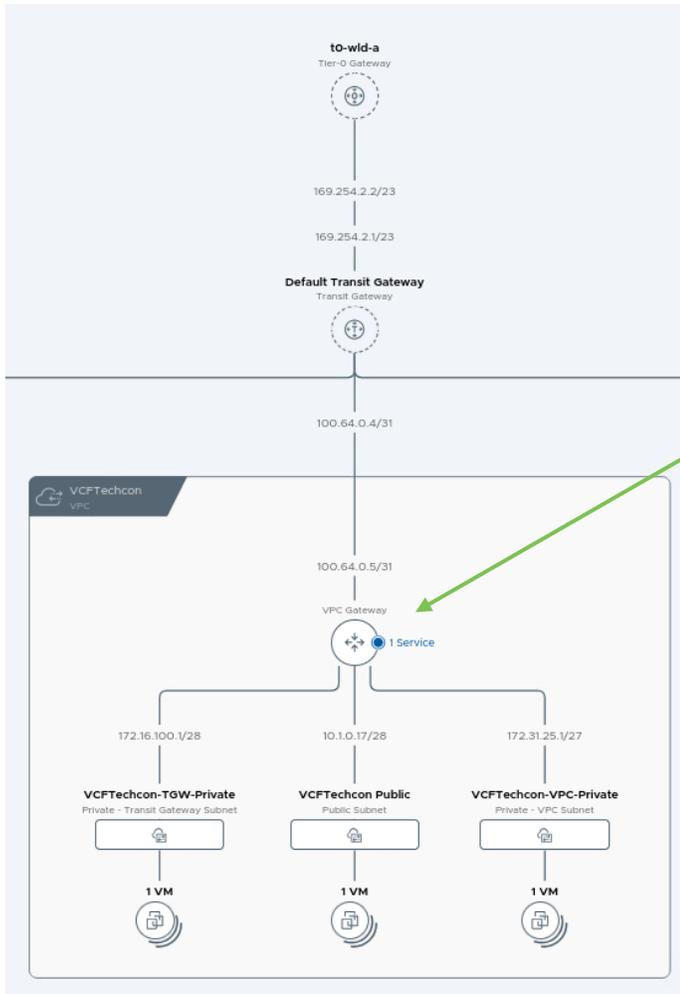
Total number of routes: 13

```
ivs> * 0.0.0.0/0 [1/0] via 169.254.2.2, inter-vrf-290, 08:03:24
t1n> * 10.1.0.0/32 [3/0] via 100.64.0.1, downlink-296, 08:03:20
t1n> * 10.1.0.1/32 [3/0] via 100.64.0.3, downlink-285, 08:03:20
t1l> * 10.1.0.2/32 [3/0] via 100.64.0.1, downlink-296, 08:03:20
t1l> * 10.1.0.3/32 [3/0] via 100.64.0.1, downlink-296, 08:03:20
t1l> * 10.1.0.4/32 [3/0] via 100.64.0.1, downlink-296, 08:03:20
t1l> * 10.1.0.5/32 [3/0] via 100.64.0.1, downlink-296, 08:03:20
t1l> * 10.1.0.6/32 [3/0] via 100.64.0.1, downlink-296, 08:03:20
t1n> * 10.1.0.7/32 [3/0] via 100.64.0.5, downlink-341, 01:00:21
t1n> * 10.1.0.8/32 [3/0] via 100.64.0.5, downlink-341, 00:22:31
t1n> * 10.1.0.9/32 [3/0] via 100.64.0.5, downlink-341, 00:22:16
t1c> * 10.1.0.16/28 [3/0] via 100.64.0.5, downlink-341, 00:57:20
t1c> * 172.16.100.0/28 [3/0] via 100.64.0.5, downlink-341, 00:55:00
```

```
edge-wld01-01a(tier0_vrf_sr[1])>
```

```
Logical Router
UUID                               VRF    LR-ID  Name                                     Type
22b4d0ed-d89f-46c6-bc03-b5fcd6fe75bf  6      1      DR-VRF-Default Transit Gateway          VRF_DISTIBU
Interfaces (IPv6 DAD Status A-DAD_Success, F-DAD_Duplicate, T-DAD_Tentative, U-DAD_Unavailable)
Interface      : 1f1f014c-76a2-5638-9864-6c4f1b848e13
Ifuid          : 341
Name           : default-VCFTechcon-t0_lrp
Fwd-mode       : IPV4_ONLY
Internal name  : downlink-341
Mode           : lif
Port-type      : downlink
IP/Mask        : 100.64.0.4/31;fceb:c5d1:9ffb:5400::1/64(NA);fe80::50:56ff:fe56:4452/64(NA)
MAC            : 02:50:56:56:44:52
VNI            : 71680
Access-VLAN    : untagged
LS_port        : 31c04648-8f90-40f3-b305-883110da193a
```

VPC routing



```
edge-wld01-01a> get gateways
Thu Oct 23 2025 UTC 18:05:21.511
Gateway
UUID                               VRF   Gateway-ID  Name                                     Type
3c36d4a2-32d9-41b0-b85d-2467ae5c7bc8  0     11          SR-t1-wld-a                             SERVICE
ce88b569-5aaa-42ae-a73b-4edbc5283743  1     13          SR-VRF-Default Transit Gateway          VRF_SE
f251a955-0046-4ea0-bc57-1349353de6c7  2     14          SR-kube-system_99ff0881-6962-452      SERVICE
5-9353-c38c22a04726
767428fe-1854-4a7e-a341-36b6305f0057  3     16          SR-vmware-system-supervisor-serv      SERVICE
ices-vpc_edfba51d-1574-4346-bf03
-65cdae69d3e2
7a858c6a-cb1f-4e1f-982e-a2f6de28ca5b  4     4           SR-t0-wld-a                             SERVICE
22b4d0ed-d89f-46c6-bc03-b5fcd6fe75bf  6     1           DR-VRF-Default Transit Gateway          VRF_DI
9cb70895-c2a1-4ab2-b07b-b2d2394771af  7     3           DR-t0-wld-a                             DISTRI
86befd84-7262-412e-a643-5ce3020ac843  8     2           DR-kube-system_99ff0881-6962-452      DISTRI
5-9353-c38c22a04726
736a80e3-23f6-5a2d-81d6-bbefb2786666  9     0           TUNNEL
aebe92cc-7970-48ec-909b-2b4f78308b1e  10    1026        SR-VCFTechcon                           SERVICE
2d58daad-4821-4542-8b92-88ea2a1ab023  11    1025        DR-VCFTechcon                           DISTRI
```

```
edge-wld01-01a> vrf 10

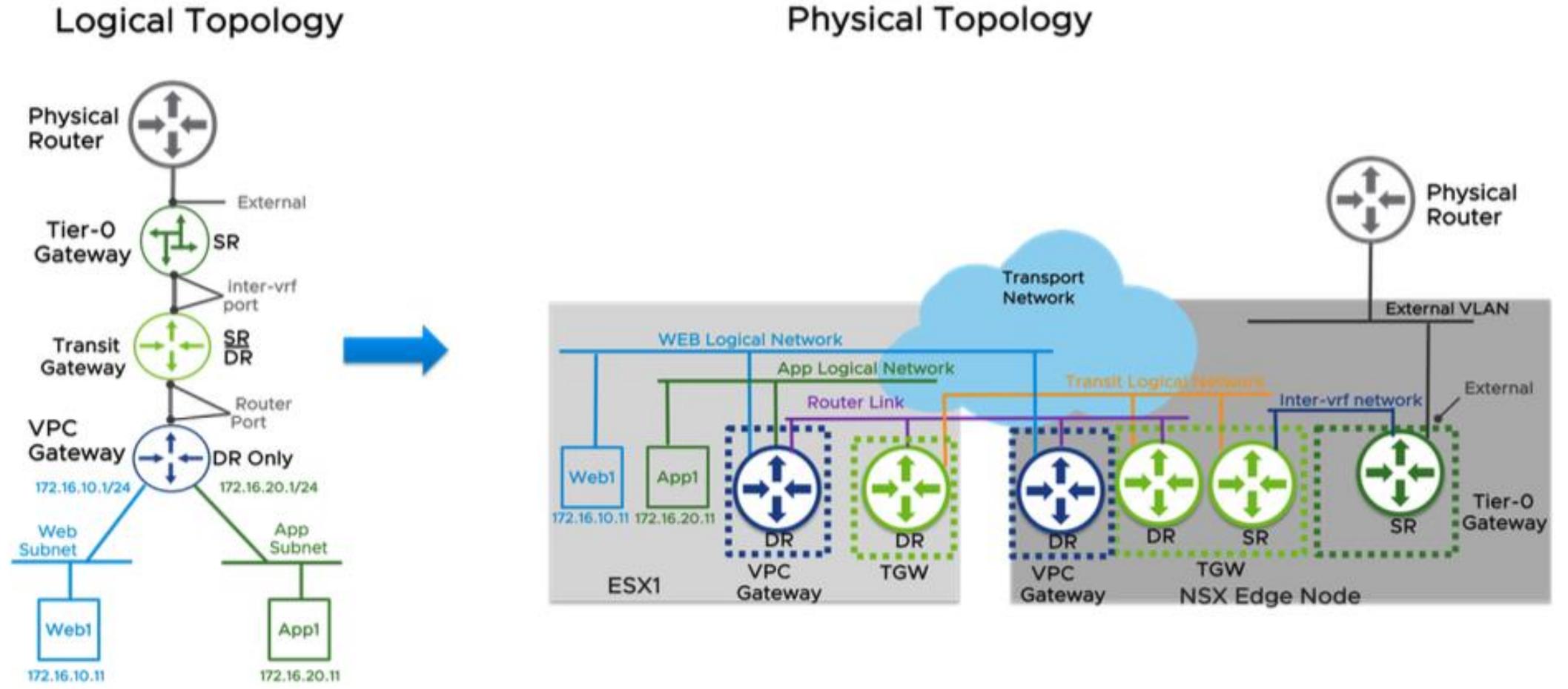
edge-wld01-01a(tier1_sr[10])> get forwarding
Thu Oct 23 2025 UTC 18:07:13.779
Logical Router
UUID                               VRF   LR-ID  Name                                     Type
aebe92cc-7970-48ec-909b-2b4f78308b1e  10    1026   SR-VCFTechcon                           SERVICE_ROUT
```

IP Prefix	Gateway IP	Type	UUID
0.0.0.0/0	100.64.0.4	route	05467a9e-5935-4270-ab0f-47
10.1.0.7/32		route	f3d95f34-7286-4a52-ba79-6c
10.1.0.16/28		route	68c46375-6f86-4032-a87d-e4
10.1.0.17/32		route	bba0382b-954c-57b2-be55-75
100.64.0.4/31		route	05467a9e-5935-4270-ab0f-47
127.0.0.1/32		route	f3d95f34-7286-4a52-ba79-6c
169.254.0.0/28		route	087230b0-4e2f-44fc-8fb1-4c
169.254.0.1/32		route	bba0382b-954c-57b2-be55-75
172.16.100.0/28		route	fff99918-3cca-47d2-a0c9-00
172.16.100.1/32		route	bba0382b-954c-57b2-be55-75
172.31.25.0/27		route	063a39b8-23bb-4dfe-a162-30
172.31.25.1/32		route	bba0382b-954c-57b2-be55-75

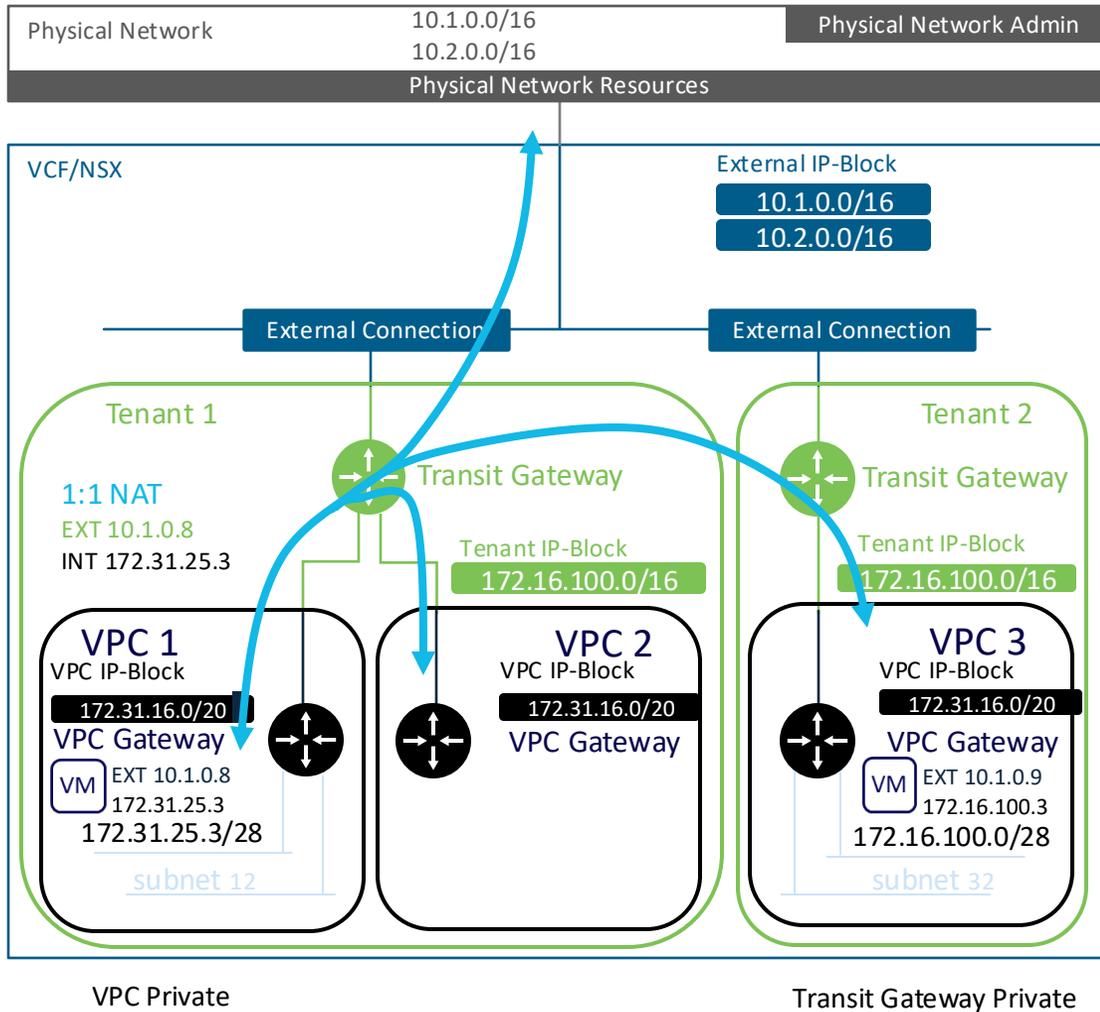
```
IPV6 Forwarding table
IP Prefix                               Gateway IP                                     Type
::/0                                     fceb:c5d1:9ffb:5400::1                       route
::1/128                                  route
fceb:c5d1:9ffb:5400::/64                route

edge-wld01-01a(tier1_sr[10])>
```

Info in the Reference Guide



VPC – External IP or 1:1 NAT



Set External IPs

VPC VCFTechcon #External IPs 2

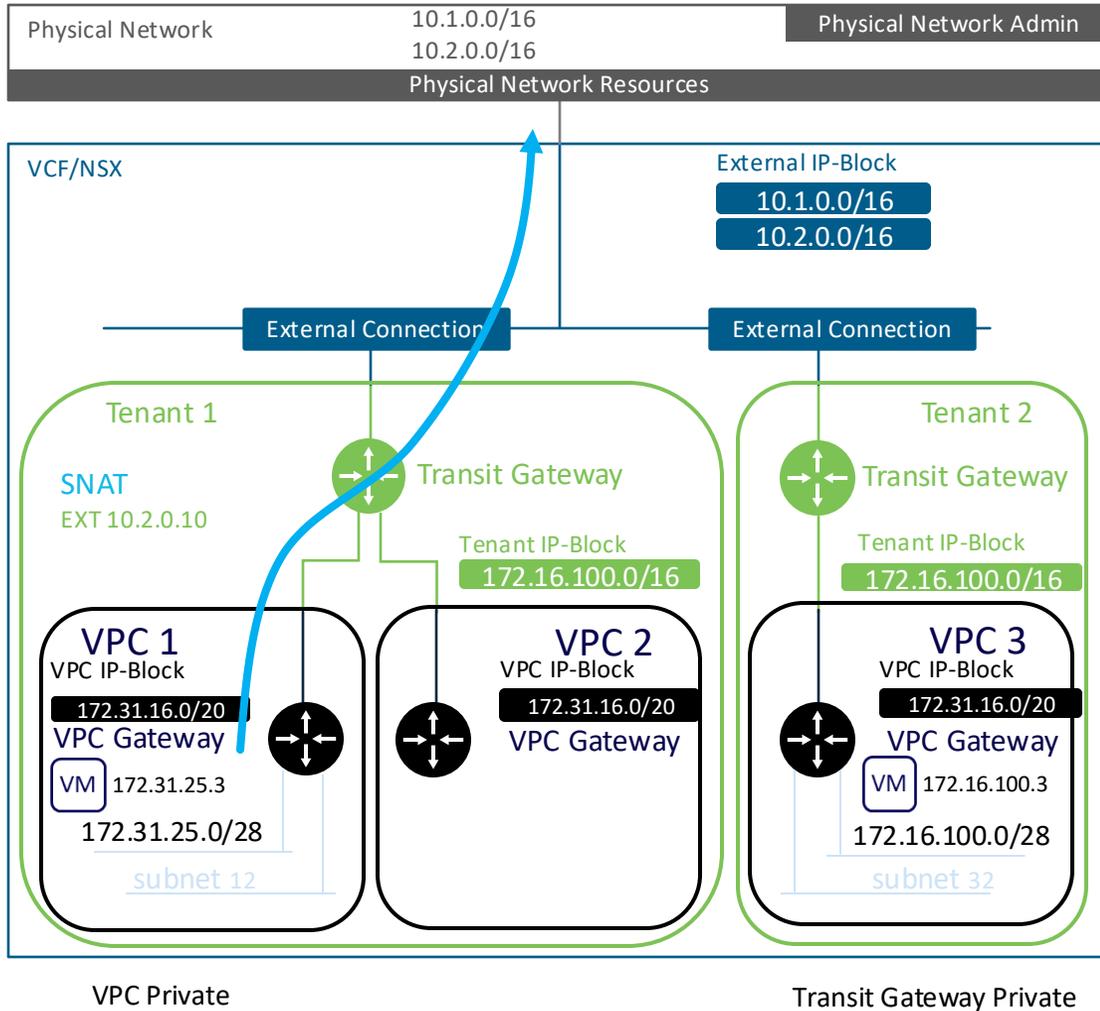
ASSIGN EXTERNAL IP

	External IP	Virtual Machine	Network Adapter	VPC Subnet	Internal IP
:	10.1.0.9	Techcon-A	Network adapter 1	VCFTechcon-TGW-Private	172.16.100.3
:	10.1.0.8	Techcon-B	Network adapter 1	VCFTechcon-VPC-Private	172.31.25.3

Uses 1 IP-address per VM

1:1 NAT
EXT 10.1.0.9
INT 172.16.100.3

VPC – Outbound NAT



Default Outbound NAT on VPC Level

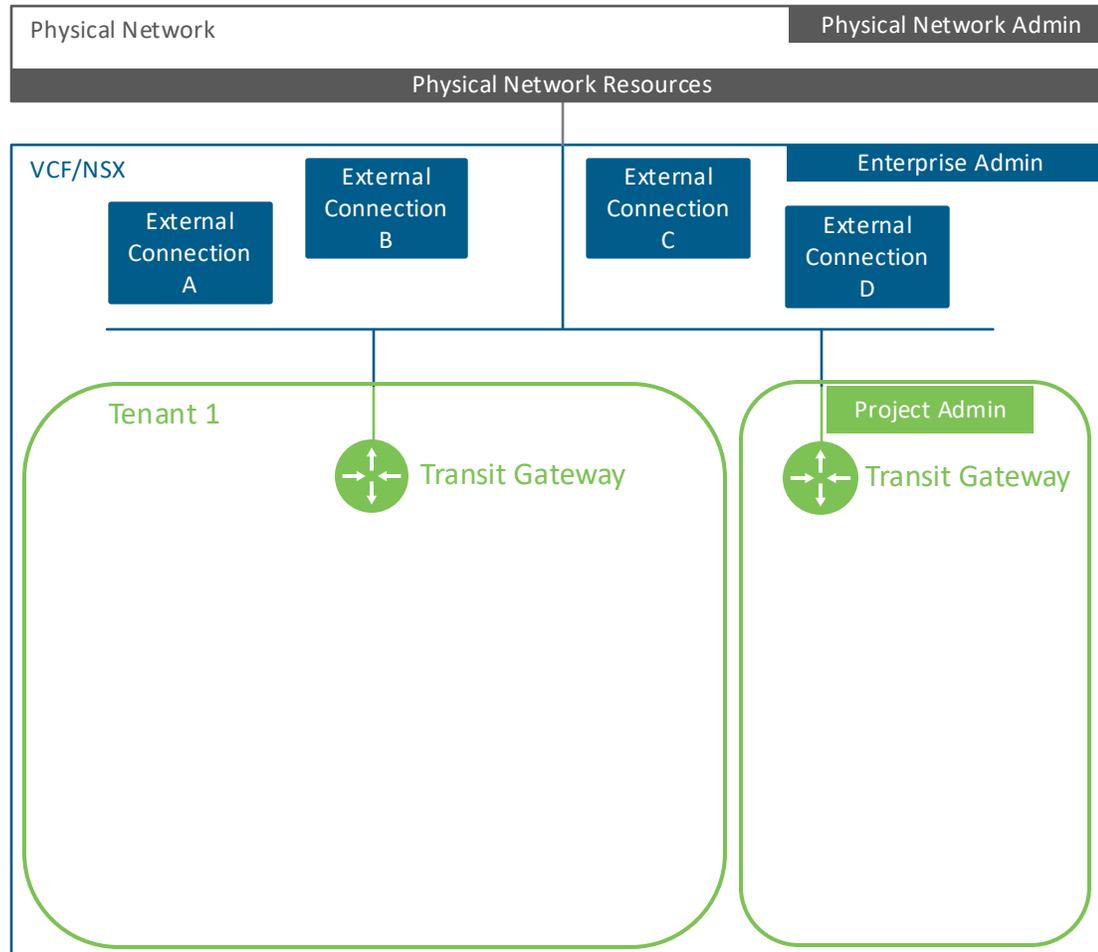


Requires A/S Transit Gateway

Uses 1 IP-address per VPC

SNAT
EXT 10.2.0.11

VCF - Transit Gateway



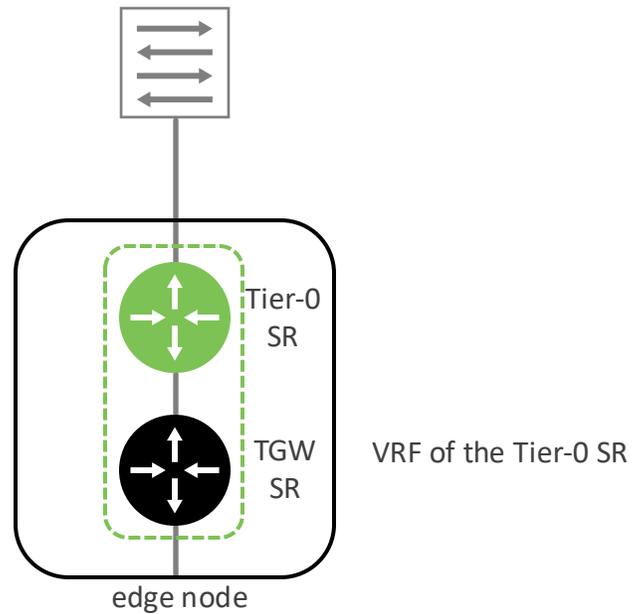
Centralized

Active/Standby

Distributed

Active/Active

VCF - Transit Gateway centralized



Configure Network Connectivity

- 1 Gateway Type
- 2 Edge Cluster
- 3 Workload Domain Connectivity
- 4 Review and Deploy

Gateway Type

Select a gateway connectivity for the created VPCs that aligns with the infrastructure requirements and networking preferences. [Learn More](#)

Centralized Connectivity

Suitable for environments where you need the full-scale of the NSX networking services.

Services: DHCP, NAT, Layer 3 services, and network monitoring and logging



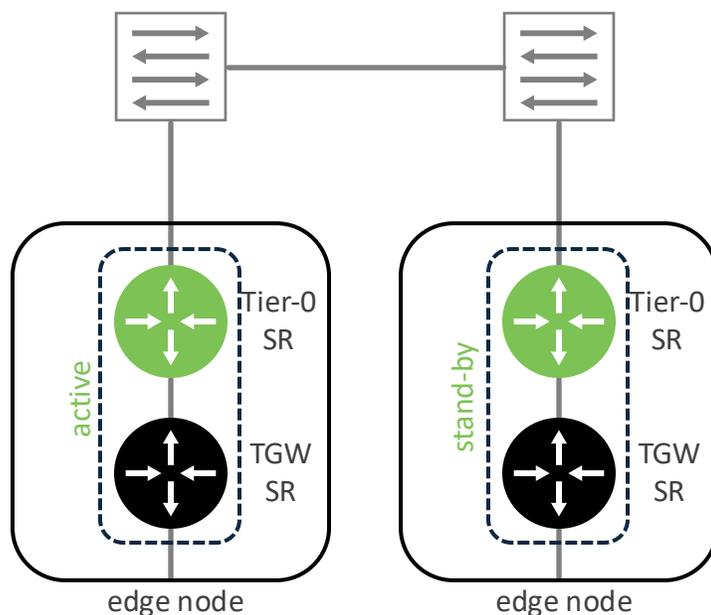
Distributed Connectivity

Suitable for environments where you need a streamlined network configuration with limited NSX networking services.

Services: DHCP, and External IP



VCF - Transit Gateway centralized A/S



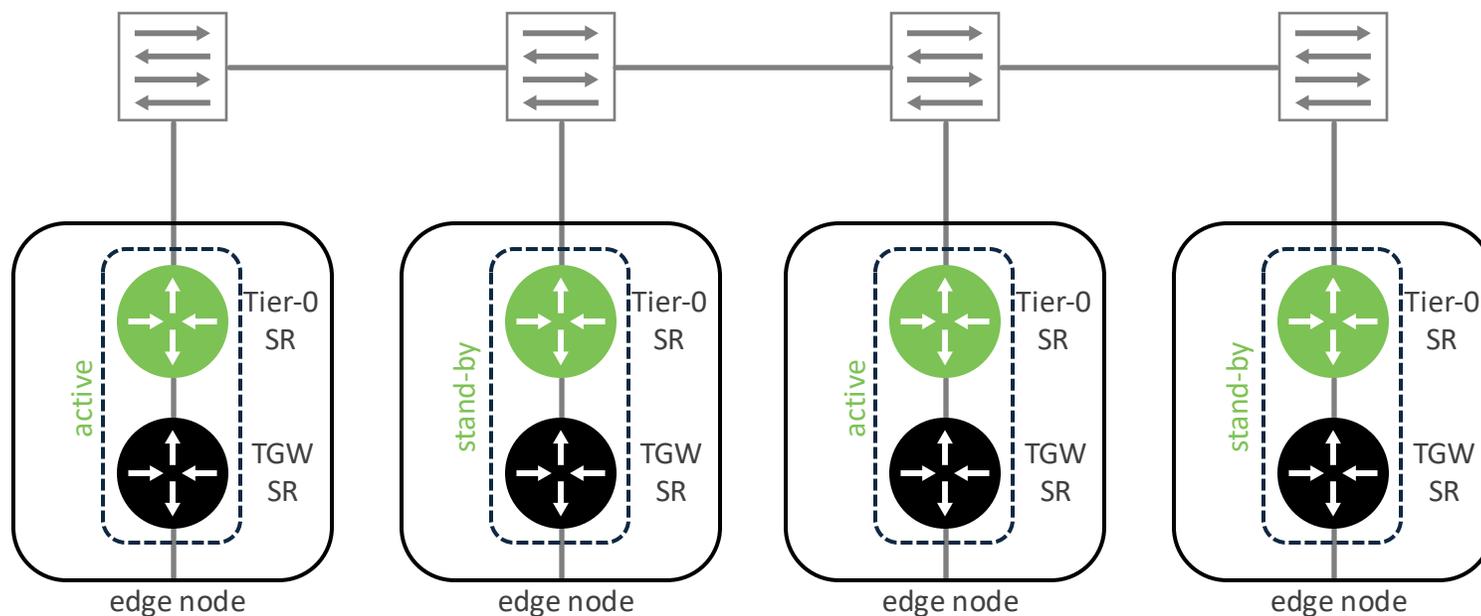
Capabilities for Centralized TGW Active/Stand-by:

- External IP (1:1 NAT)
- VPC Default Outbound NAT
- NAT (SNAT/DNAT)
- N/S Firewall
- E/W Firewall
- AVI Load Balancer
- DHCP

Active/Stand-by Centralized TGW is required for:

- Supervisor cluster (VKS)
- VCF Automation modern experience

VCF - Transit Gateway centralized A/A



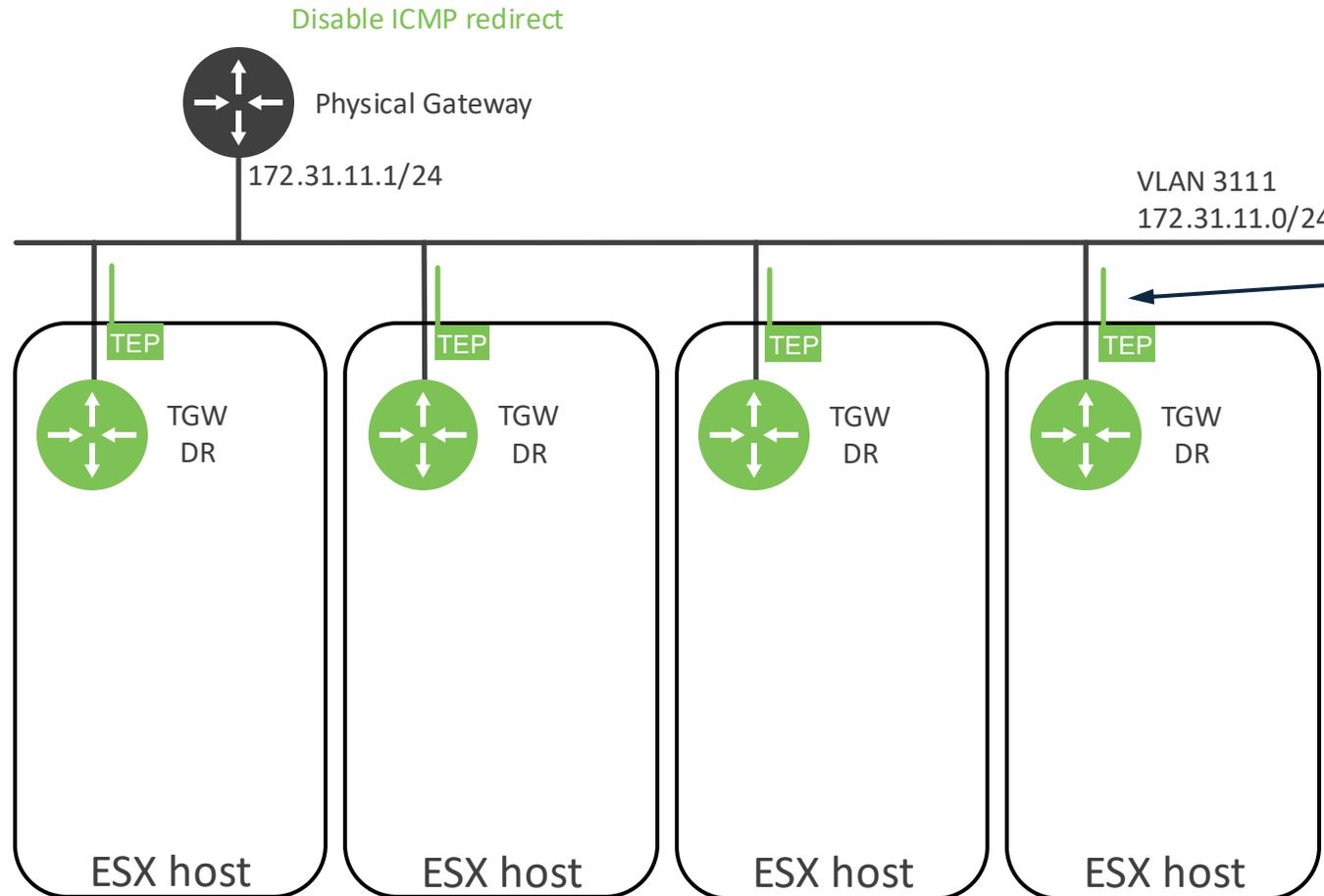
Capabilities for Centralized TGW Active/Active:

- External IP (1:1 NAT)
- NAT (SNAT/DNAT)
- E/W Firewall
- DHCP
- AVI Load Balancer

Cannot run

- VPC Default Outbound NAT
- N/S Firewall

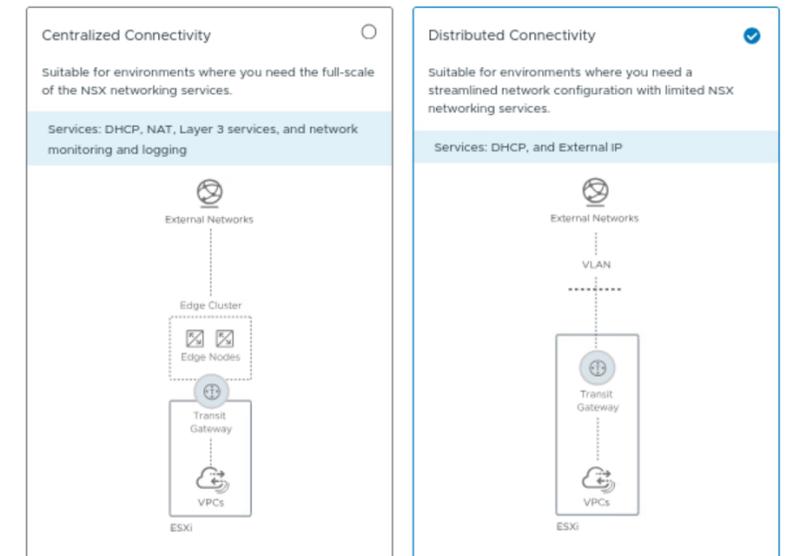
VCF - Transit Gateway distributed



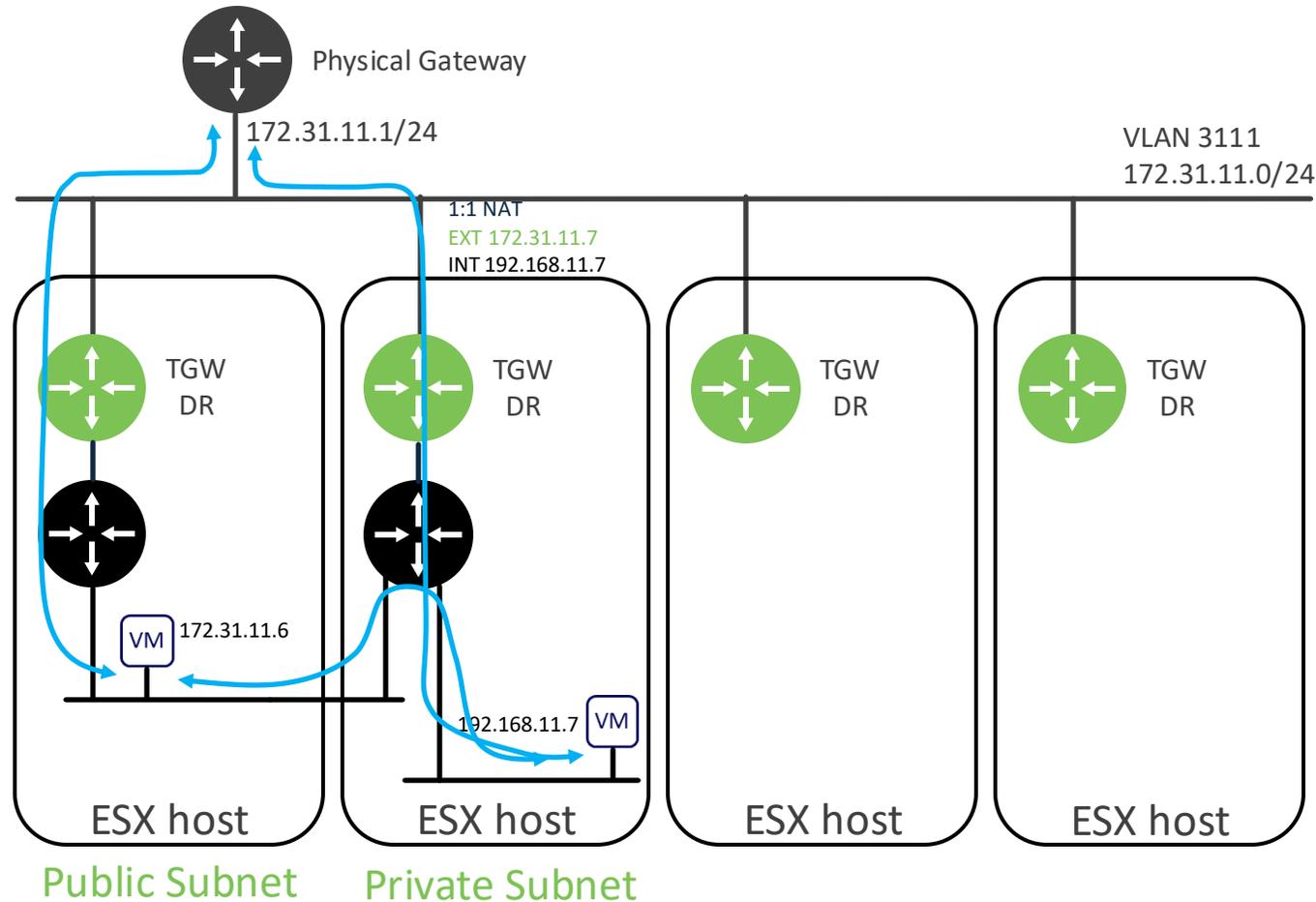
The uplink where the TEP is located will be used and must be connected to external VLAN e.g. 3111

Gateway Type

Select a gateway connectivity for the created VPCs that aligns with the infrastructure requirements and networking preferences. [Learn More](#)



VCF - Transit Gateway distributed



VPC with Distributed TGW allows the following capabilities:

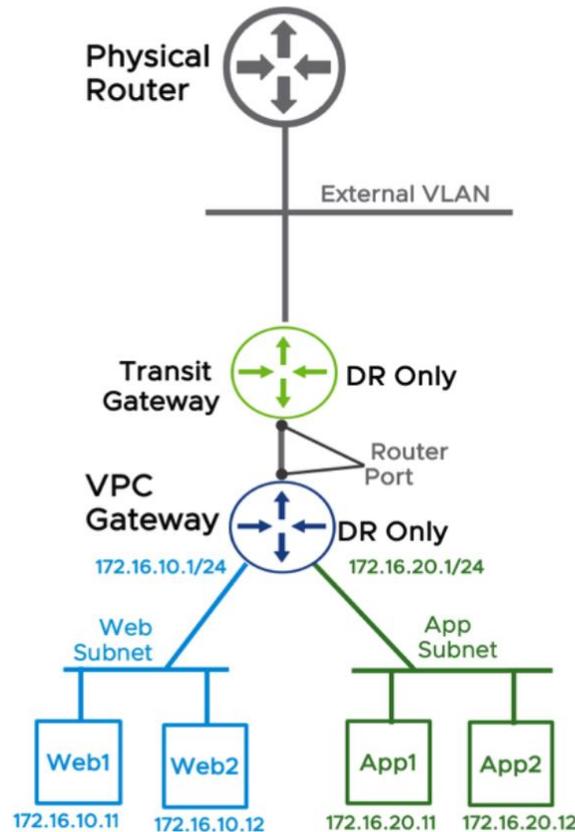
- External IP (1:1 NAT)
- E/W Firewall
- Distributed DHCP
- AVI Load Balancer
(no client IP transparency support)

Does not allow the following capabilities:

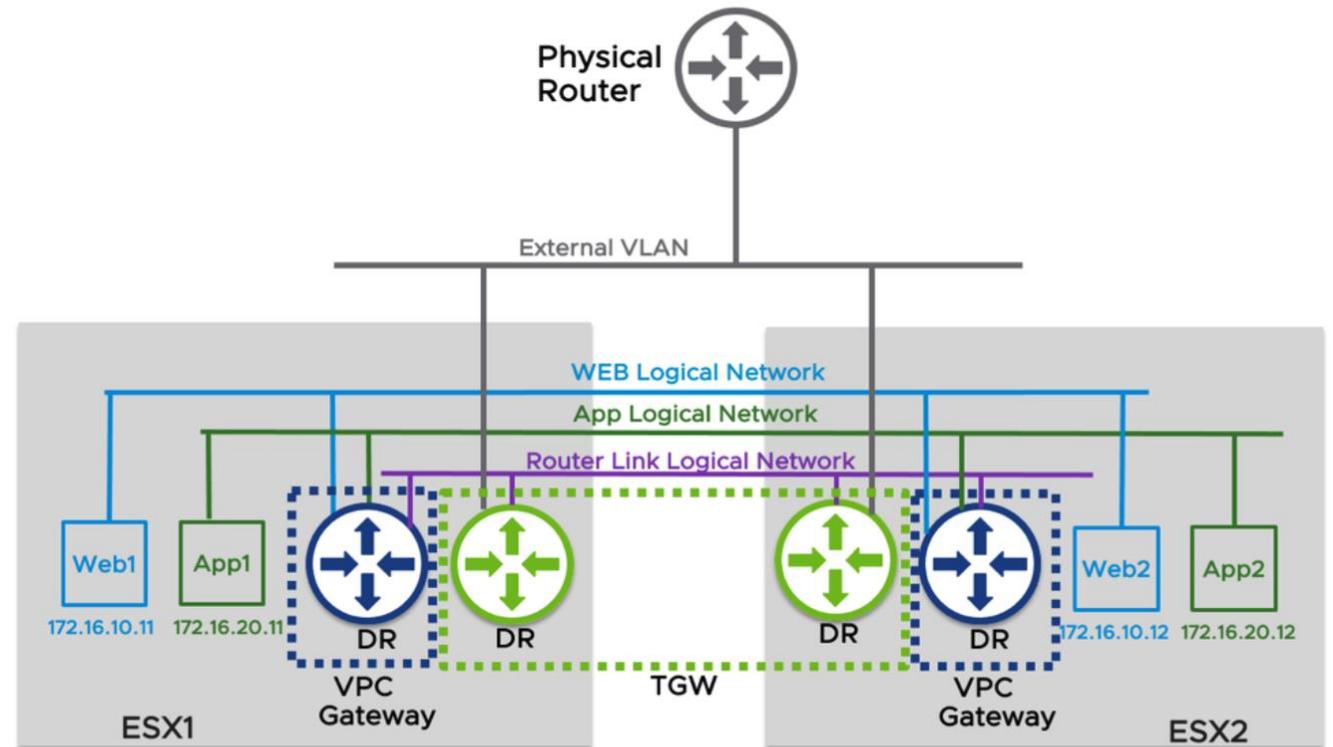
- VPC Default Outbound NAT
- NAT (SNAT/DNAT)
- N/S Firewall

VCF - Transit Gateway distributed

Logical Topology

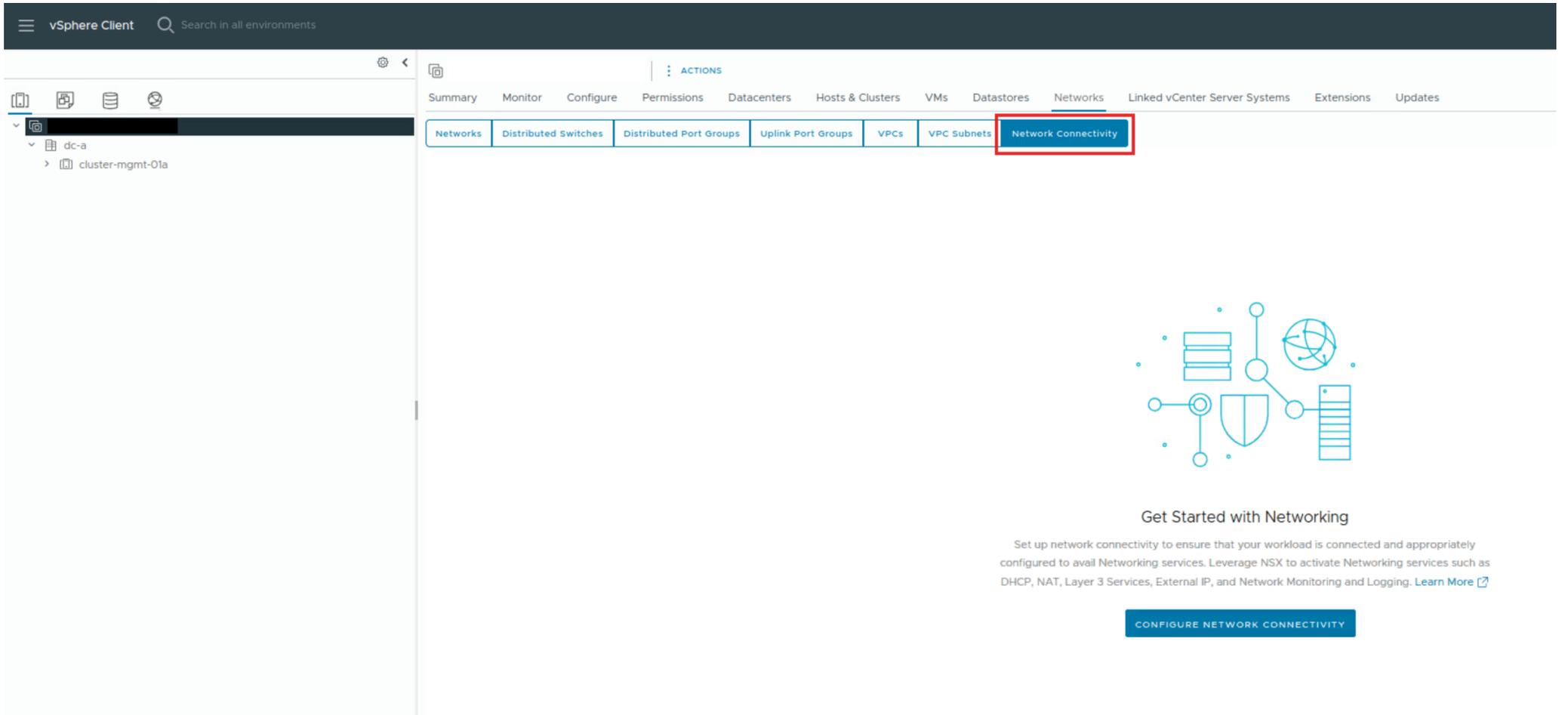


Physical Topology



Transit Gateway distributed

- Enabled from vCenter



The screenshot displays the vSphere Client interface. The top navigation bar includes the vSphere Client logo and a search field. Below this, a breadcrumb trail shows the path: Summary > Monitor > Configure > Permissions > Datacenters > Hosts & Clusters > VMs > Datastores > Networks > Linked vCenter Server Systems > Extensions > Updates. The 'Networks' tab is selected, and a sub-menu is open, highlighting 'Network Connectivity' with a red box. The left sidebar shows a tree view with 'dc-a' expanded to show 'cluster-mgmt-01a'. Below the navigation, there is a section titled 'Get Started with Networking' with a blue icon representing network connectivity. The text below the icon reads: 'Set up network connectivity to ensure that your workload is connected and appropriately configured to avail Networking services. Leverage NSX to activate Networking services such as DHCP, NAT, Layer 3 Services, External IP, and Network Monitoring and Logging. [Learn More](#)'. A blue button labeled 'CONFIGURE NETWORK CONNECTIVITY' is positioned at the bottom right of this section.

Transit Gateway distributed

The screenshot displays the AWS Transit Gateway configuration console. The main window is titled "Configure Network Connectivity" and is divided into two sections: "1 Gateway Type" and "2 External Network Connectivity".

Gateway Type

External Network Connectivity

Please provide networking details for external connectivity to your TOR. [Learn More](#)

VLAN ID Value from 0 to 4094

Gateway CIDR IPv4 Address Gateway IP CIDR will also configure External IP Blocks for VPCs. e.g. 10.10.10.1/24

VPC Configuration

VPC External IP Blocks Provide External IPs to setup external connectivity for VPC. e.g. 10.10.10.0/24

Private - Transit Gateway IP Blocks Provide Private IPs for VPC configuration. e.g. 172.16.10.0/24

Networking Prerequisites

Complete the required prerequisites

- Select All
- Dedicated VLAN(s) and subnets must running VPC workloads must have access to these VLANs forwarded back to same
- Disable 'ICMP redirect' on external gateway
- Reserve external IP block(s) for VPC connectivity

External Networks

Distributed Gateway

VPCs

CANCEL **BACK** **DEPLOY**

Transit Gateway capabilities

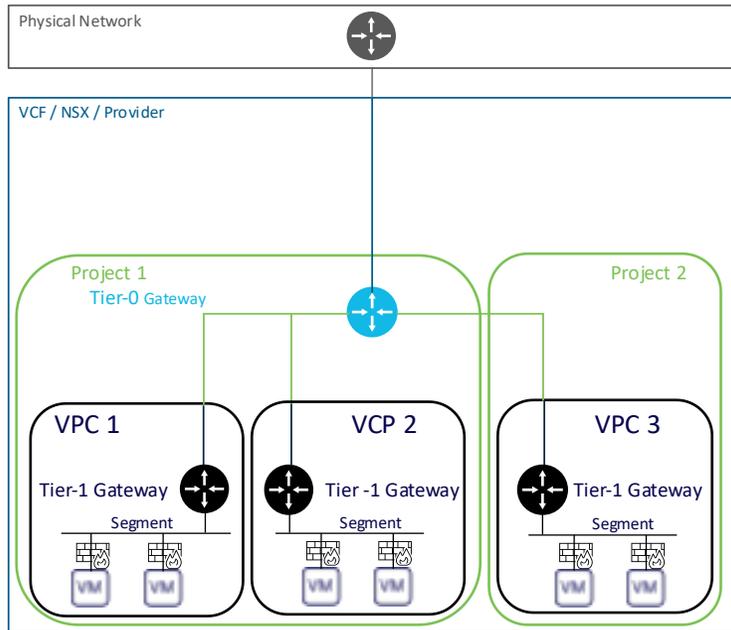
Centralized Active/Standby	Centralized Active/Active	Distributed
External IP (1:1 NAT)	External IP (1:1 NAT)	External IP (1:1 NAT)
NAT (SNAT/DNAT)	NAT (SNAT/DNAT)	Not available
VPC Default Outbound NAT	Not available	Not available
DHCP	DHCP	Distributed DHCP
E/W Firewall	E/W Firewall	E/W Firewall
N/S Firewall	Not available	Not available
AVI Load Balancer	AVI Load Balancer	AVI Load Balancer (no client IP transparency support)
A/S Centralized TGW is required for: Supervisor cluster (VKS) VCF Automation modern experience		

Current VPC limitations in VCF 9.0

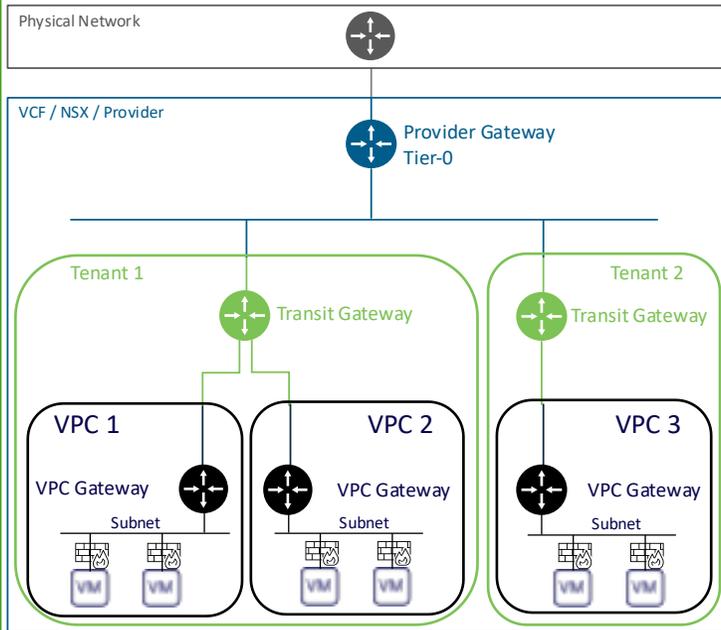
- Bridging to VLAN (no access to physical infrastructure)
- Multicast routing
- IPv6 routing
- Federation

VPC – Networking models

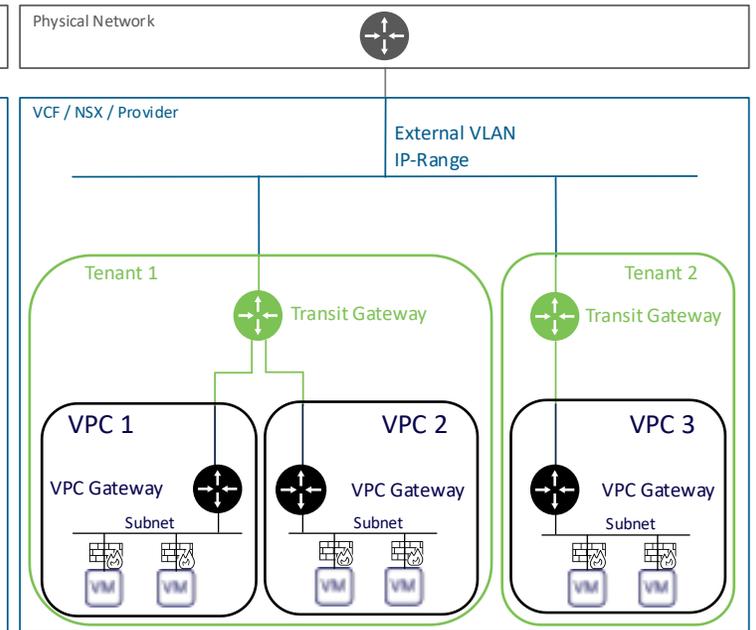
Segment Networking model



VCF Networking models



Central Transit Gateway



Distributed Transit Gateway

NSX Networking Models compared

Networking Model	NSX Objects	Capabilities
Segment Network model	<ul style="list-style-type: none">• Tier-0 Gateways• Tier-1 Gateways• Segments• East-West Distributed Firewall• North-South Gateway Firewall• Nat Rules	<ul style="list-style-type: none">• NSX Federation• Centralized management model• Self-service via NSX multi-tenancy (Projects)• VPNs on Tier-0 and Tier-1 Gateways• VCF Automation can discover NSX Segments (Cloud users can only connect workloads)
VPC Network Model	<ul style="list-style-type: none">• Provider Gateways (Tier-0)• Transit Gateways• VPC's• Subnets• East-West Distributed Firewall• North-South Gateway Firewall• External Ips• Nat Rules	<ul style="list-style-type: none">• Embedded IPAM• vCenter UI intergration• Self-service or Centralized management model• VPNs of Tier-0 only• Cloud users can create VPC and Subnets and connect workloads via VCF Automation

VCF – Config Edge Nodes

- Deploy Edge nodes from vCenter

Configure Edge Node

Edge Node Name (FQDN) *
e.g. example.domain.com

vSphere Cluster *
Cluster for the deployment of NSX Edge node

Resource Pool

Host Group Affinity ⓘ Yes No

Data Store *

Management IP

Management network details for the Edge node

IP Allocation DHCP Static

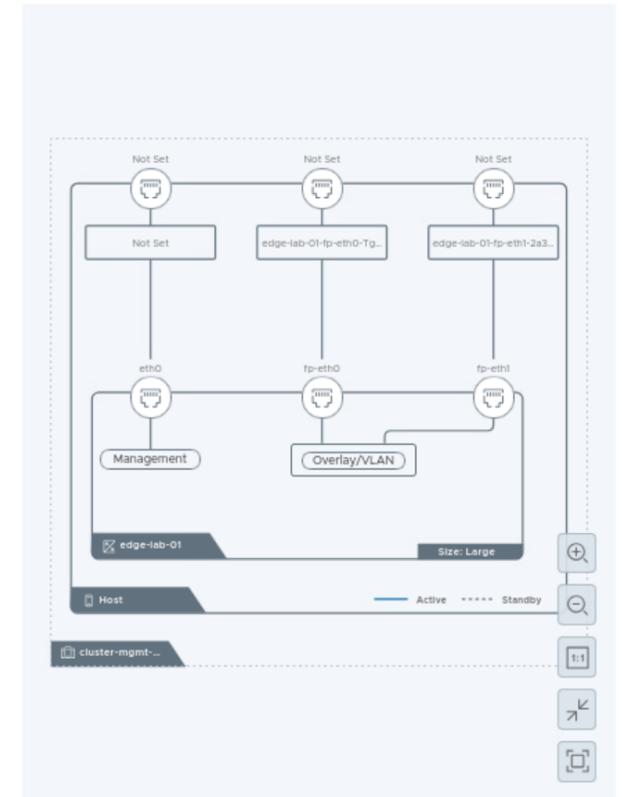
Port Group * ⓘ

Uplinks

Use the host overlay network configuration from the selected vSphere Cluster ⓘ

Edge Node Uplink Mapping

Virtual Interfaces	Interfaces	Active PNICs	Standby PNICs
1	fp-eth0	<input type="text" value="Select PNIC"/> ⓘ	<input type="text" value="Select PNIC"/> ⓘ
2	fp-eth1	<input type="text" value="Select PNIC"/> ⓘ	<input type="text" value="Select PNIC"/> ⓘ



CANCEL

APPLY

Vragen?