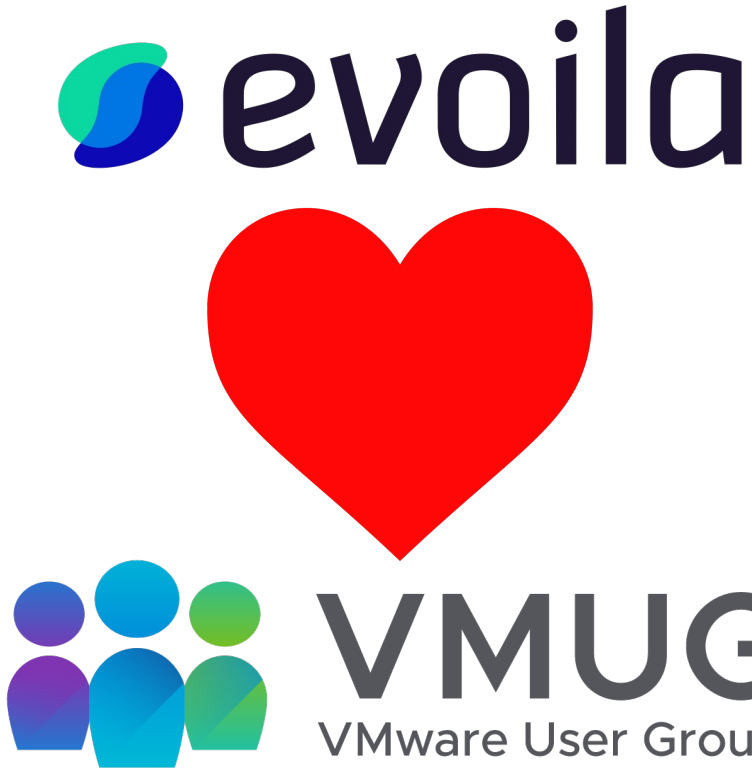

evoila
VMUG
VMware User Group

VPC Networking in VCF 9 / NSX

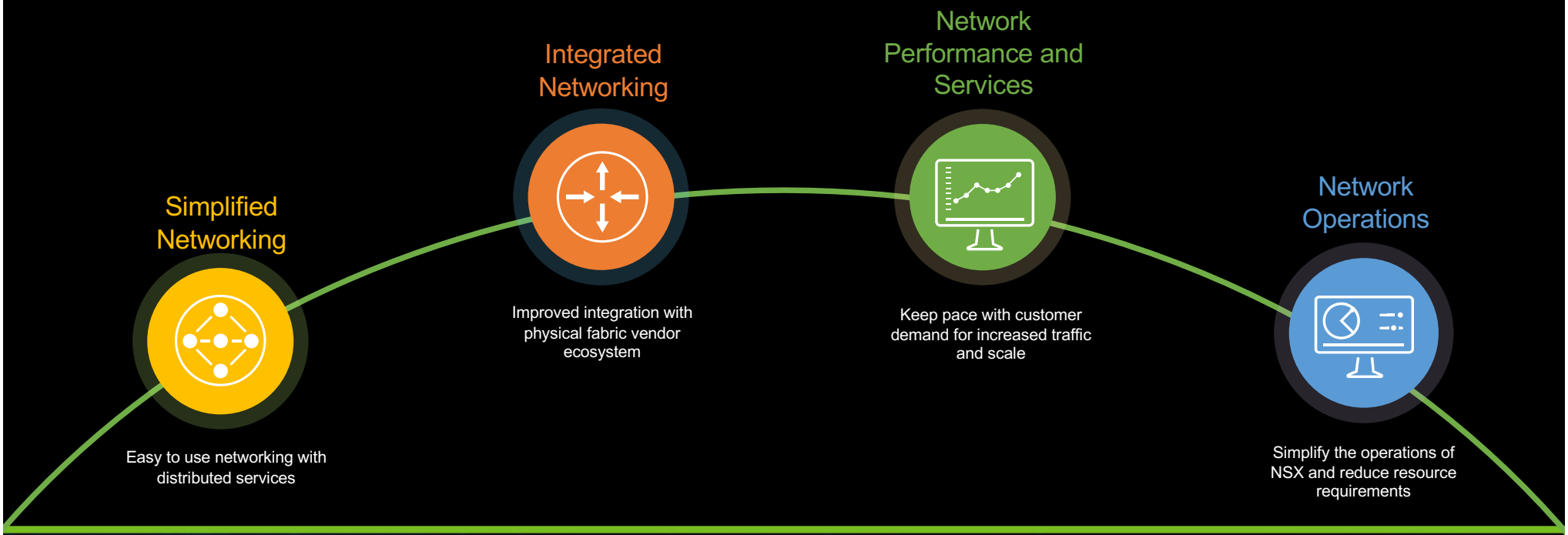
Daniel Krieger aka SDN-Warrior

- Blogger (sdn-warrior.org)
- Homelabber
- vExpert
- Broadcom VCF Knight
- Cloud Architect @ evoila

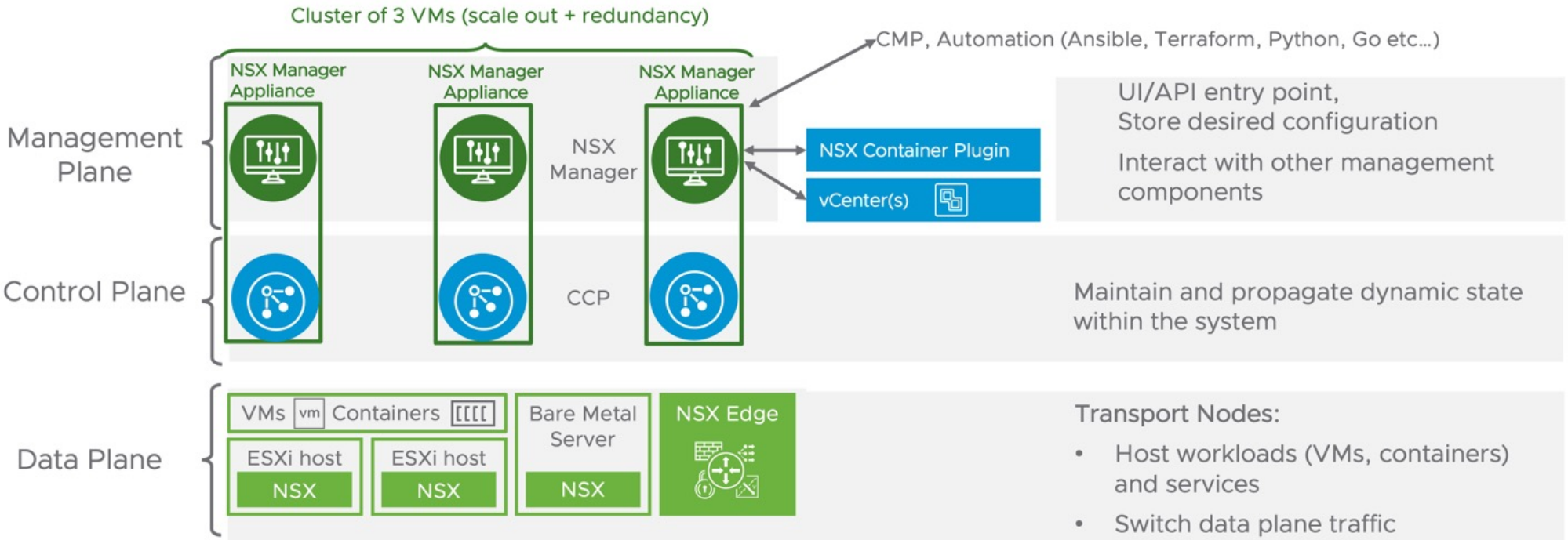
Agenda

- Overview NSX and VPCs
- Demo
- Technical fundamentals of VPCs
- Q & A

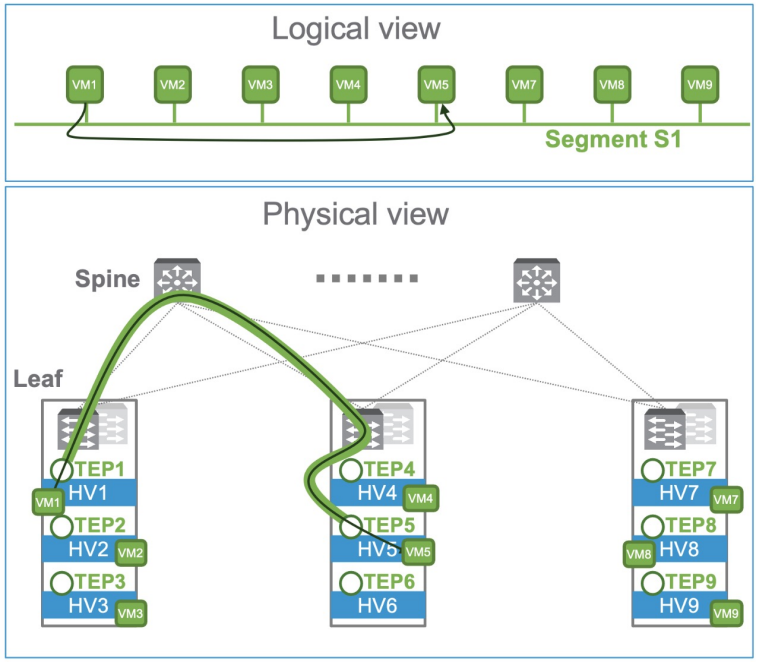
NSX aka VCF Networking



NSX Architecture

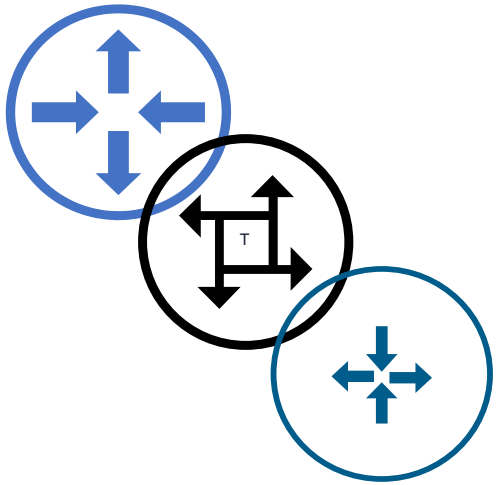


Segments



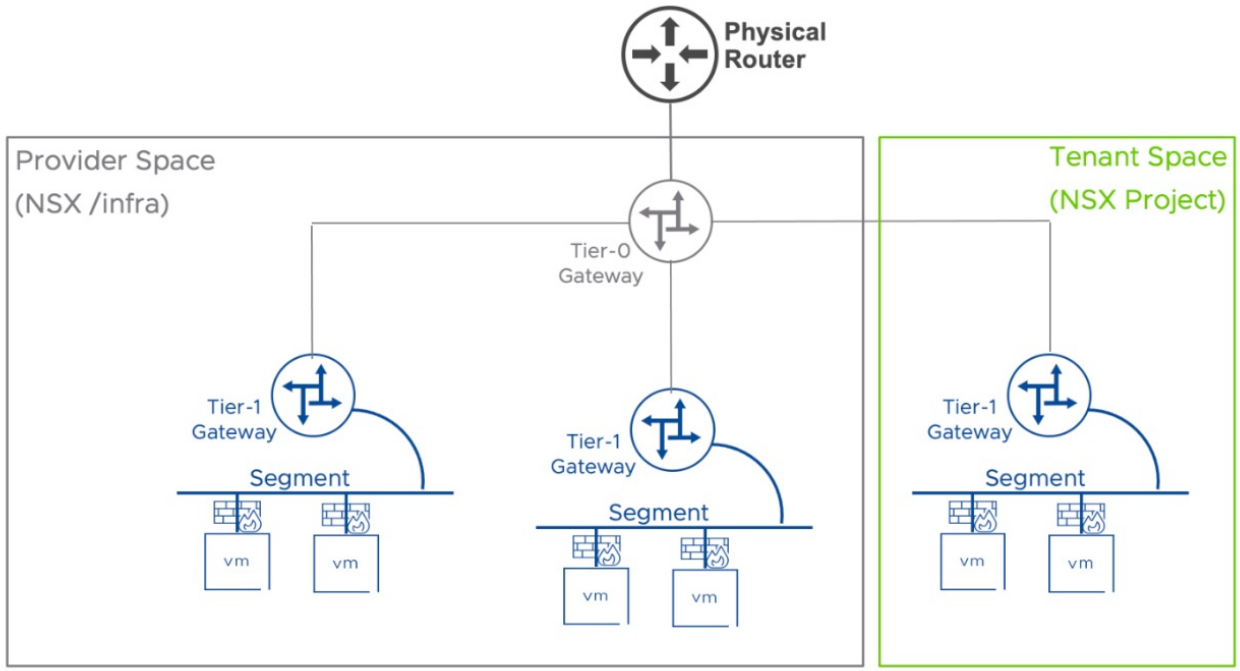
- Layer 2 Domain
- Overlay
- VLAN
- May be on one or neither of the T1/T0 routers

Gateways



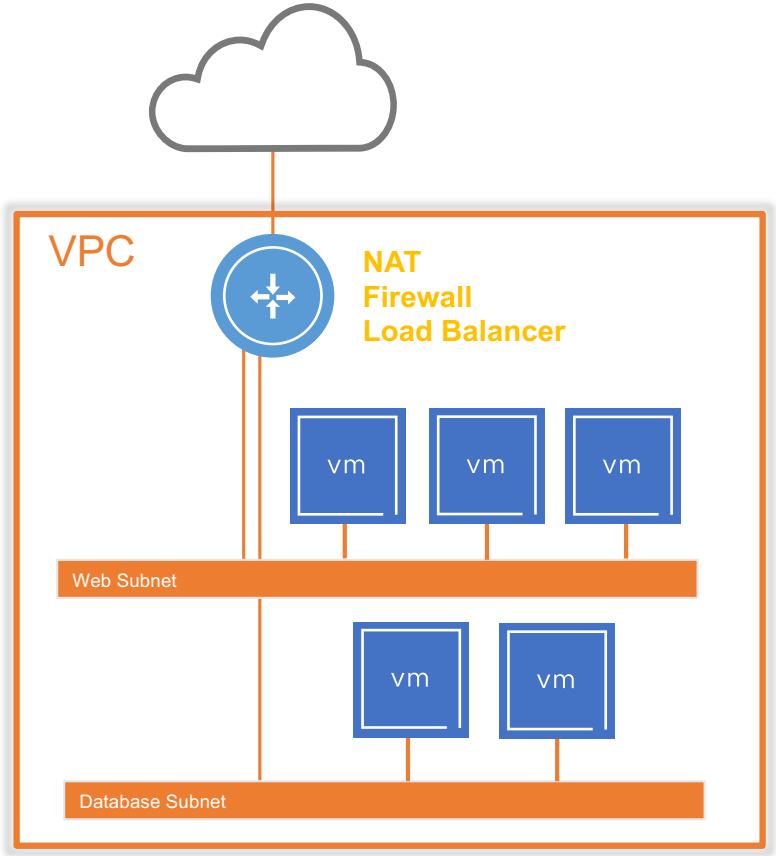
- T0 Router
  - North/South Traffic
  - BGP/OSPF/Static Routing
- T1 Router
  - East/West Routing
  - Stateful Services
- Transit Gateway
  - External Connection for VPCs
- VPC Gateway
  - East/West Routing for VPCs

NSX Projects

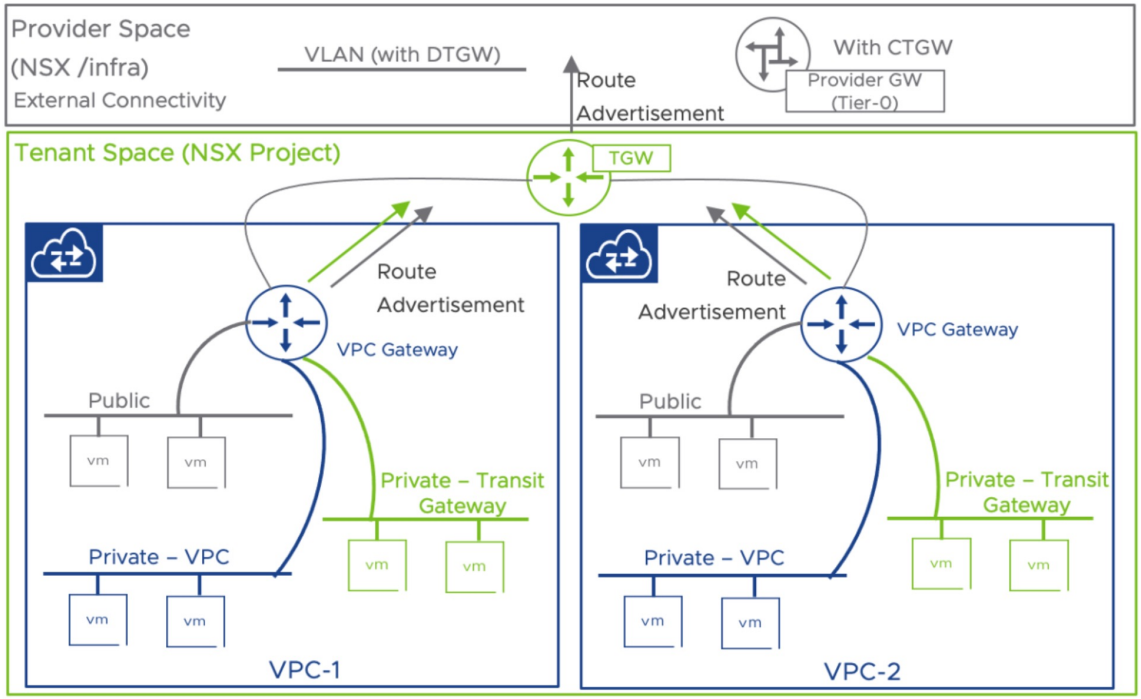


VPCs in VCF9

1. Subnets
2. IP Gateway
3. Network Services

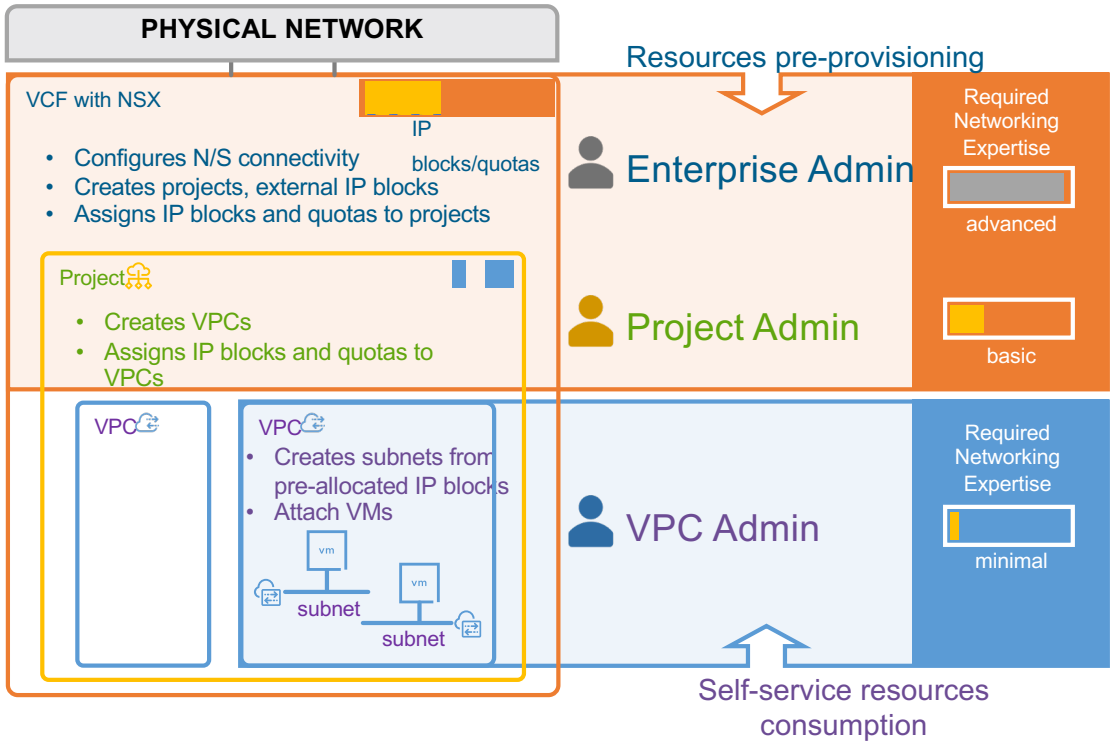


VPC Subnet Types



- Public (Grey)
  - Public subnets provide direct routability
- Private – VPC (Blue)
  - Private VPC subnets are strictly routable within their own VPC boundary
- Private – Transit (Green)
  - Private TGW (Transit Gateway) subnets enable routing
  - between multiple VPCs connected to the same Transit Gateway

Role definition

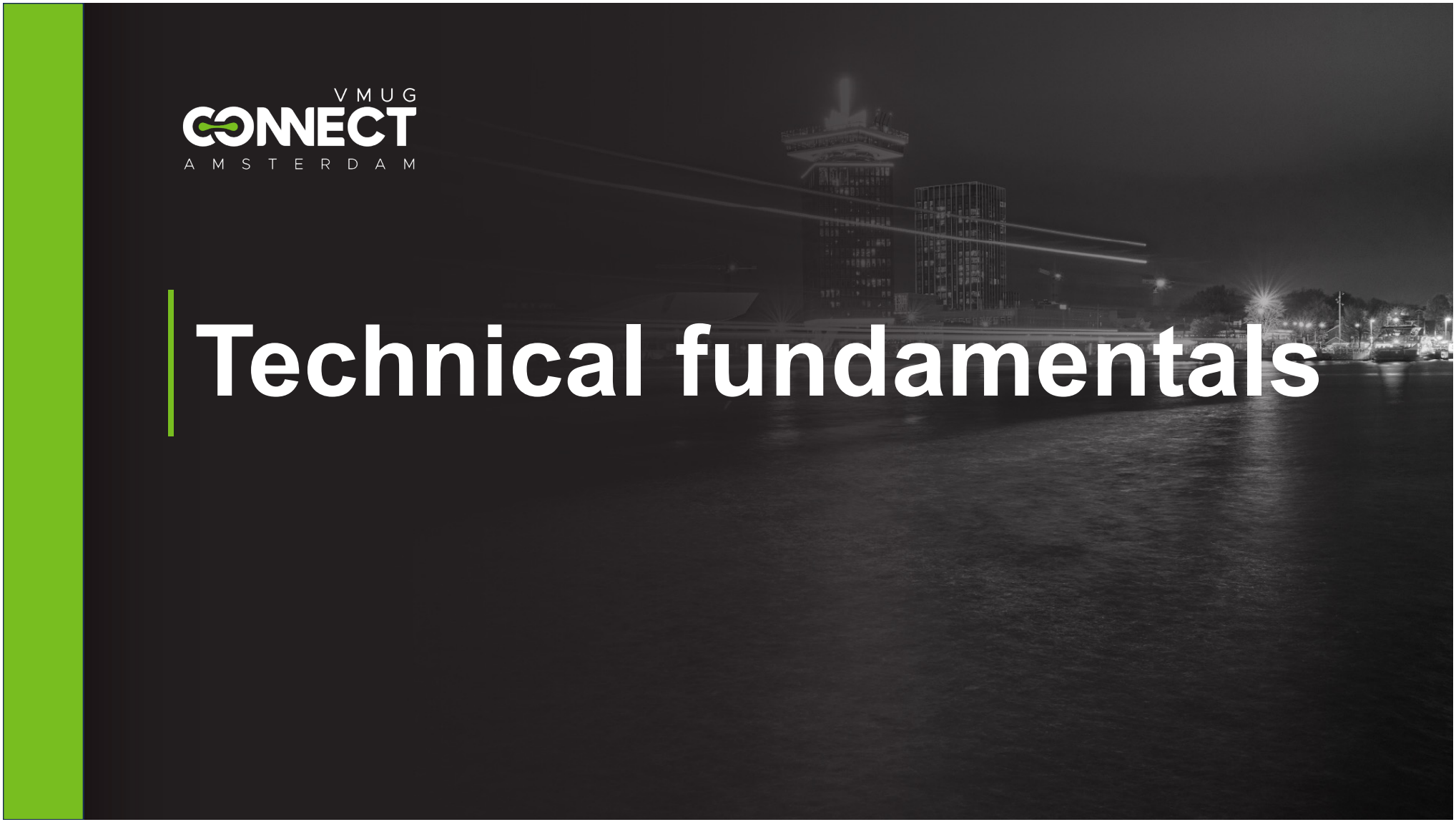


- Enterprise Admin
  - Owns the physical infrastructure
- Project Admin
  - A tenant
  - No direct access to physical network
- VPC Admin
  - End user
  - Simple, self-service networking

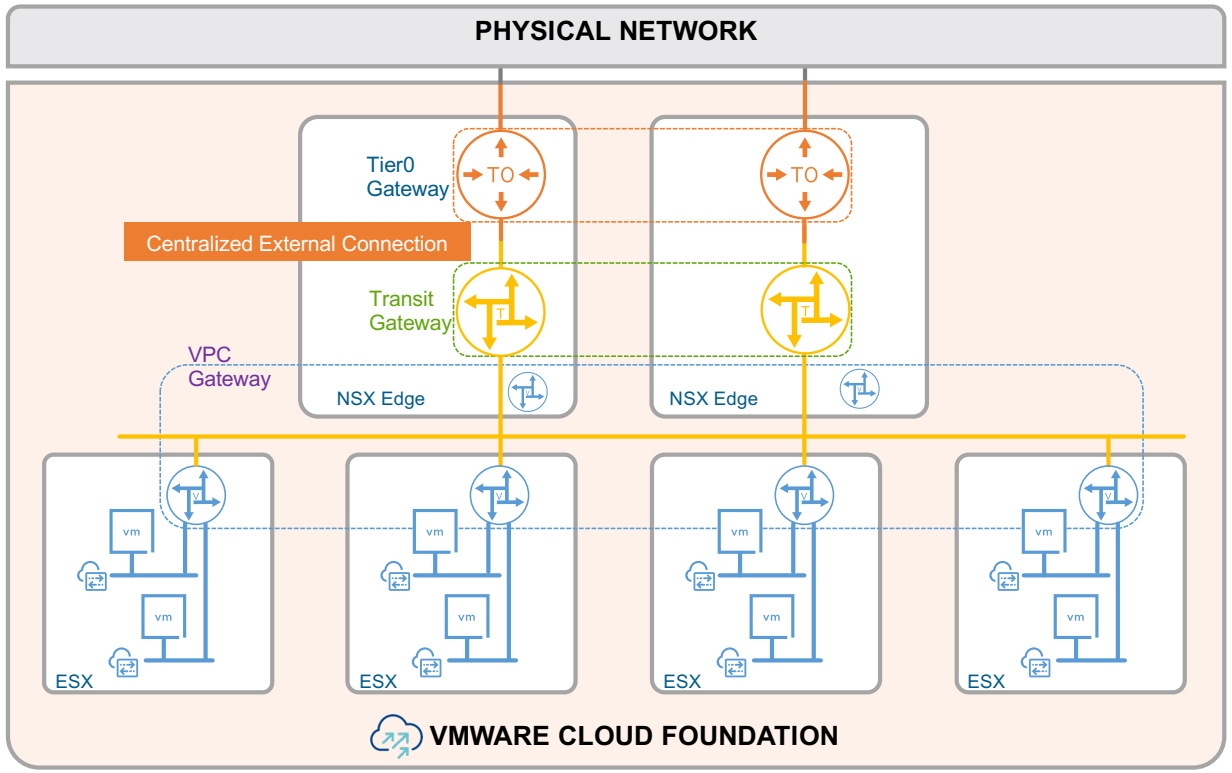
Key Benefits of VPCs

- **Multi-tenancy**
  Secure isolation of multiple tenants or business units
- **Simplified Management**
  Streamlined operations with same pane of glass as compute and storage
- **Scalability**
  Easy expansion and customization to accommodate growth
- **Components Support**
  Supports many VCF components such as VKS, VCF Automation, and AVI Advanced Load balancer. Full NSX Terraform Provider support.


VMUG
CONNECT
AMSTERDAM
Live Demo
(Fingers crossed)


VMUG
CONNECT
AMSTERDAM
Technical fundamentals

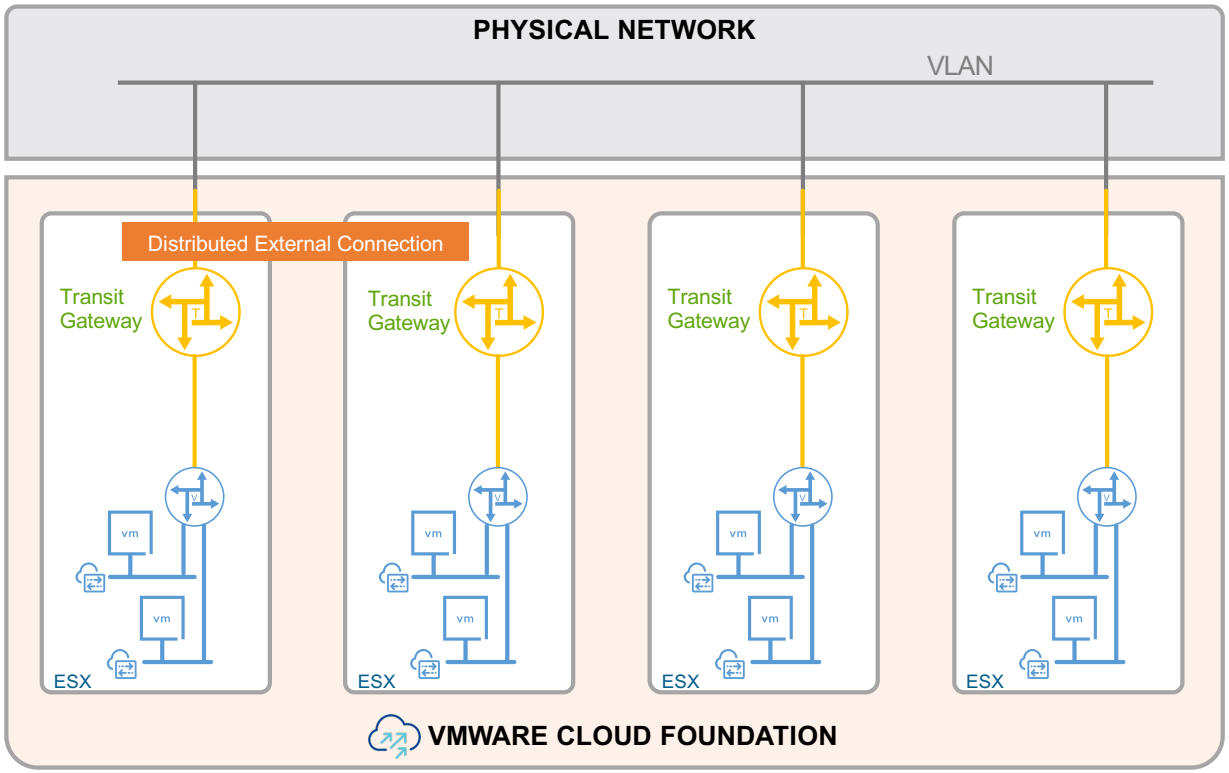
Transit Gateway Centralized



NSX edges required

- NAT
- DHCP
- QoS profiles
- Gateway firewall (with license)
- Supervisor cluster and VCF automation modern experience

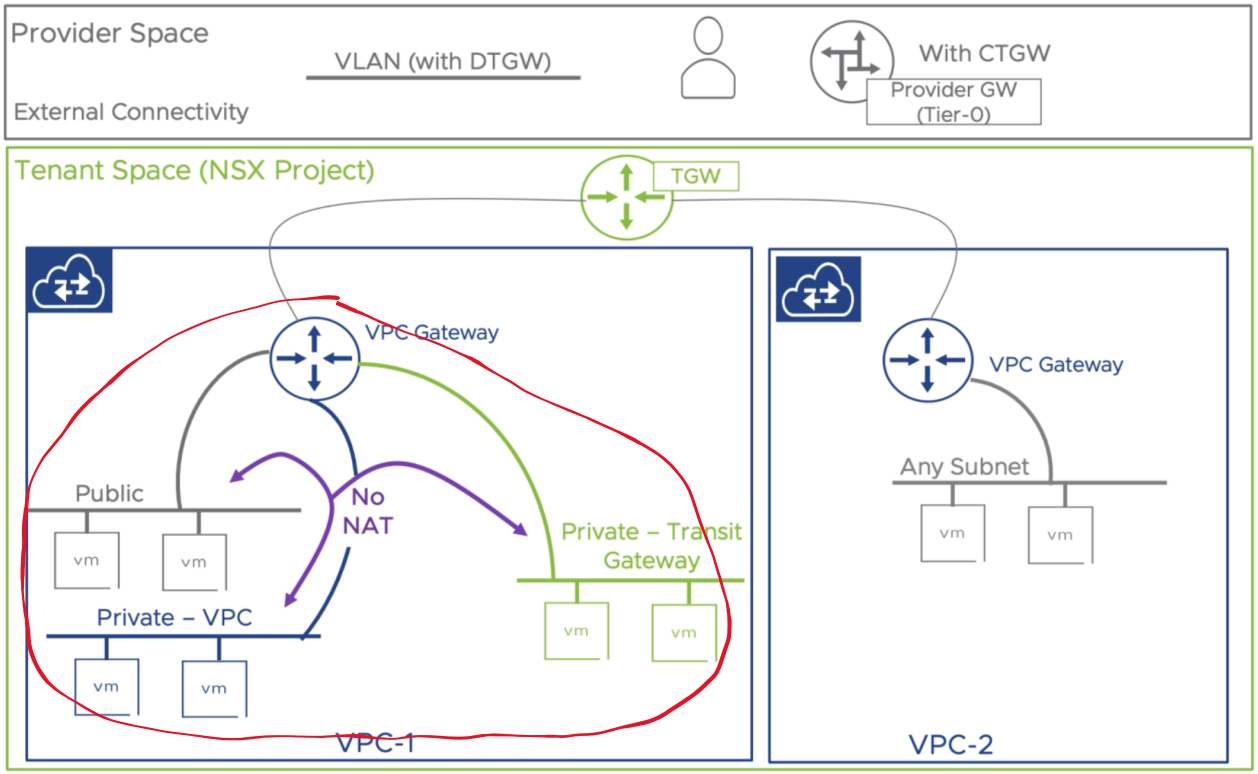
Transit Gateway Distributed



No NSX edges

- All ESX hosts must be connected to a VLAN providing an IP block for external addresses used by VMs
- Distributed services:
- 1:1 NAT (reflexiv)
- distributed DHCP

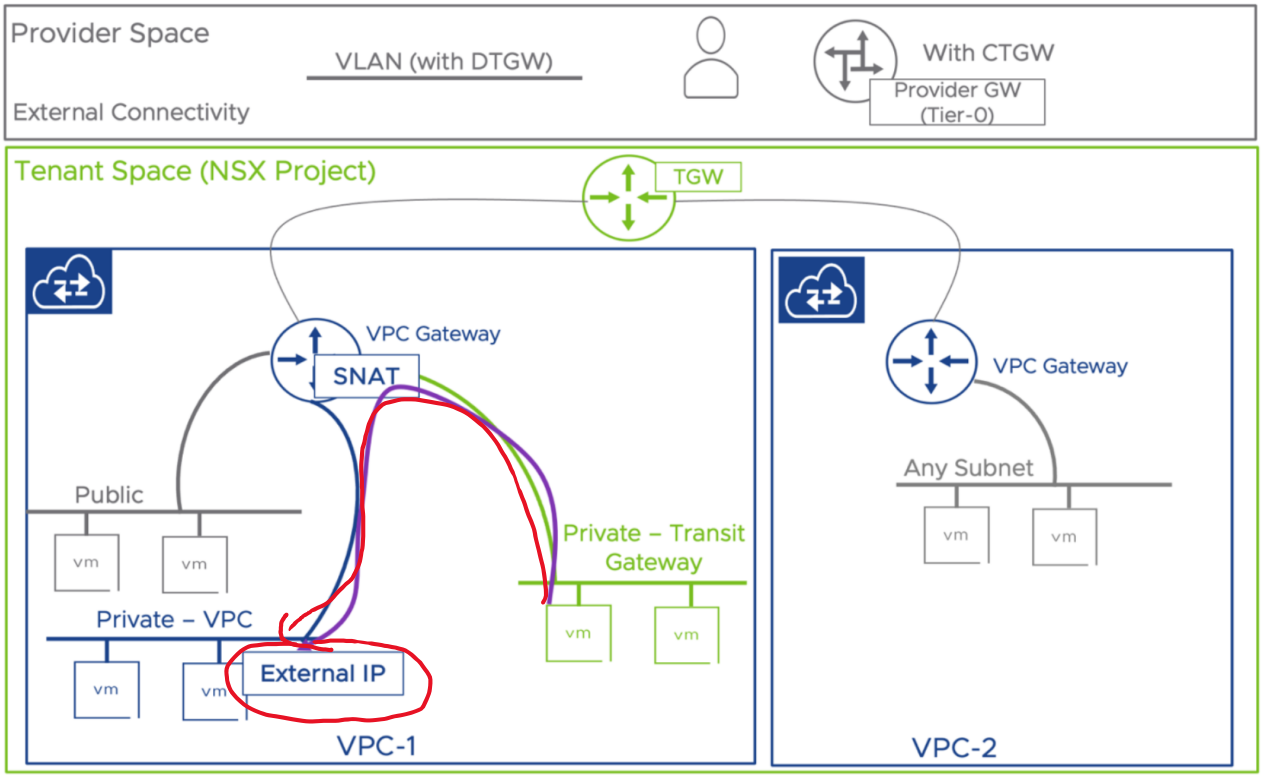
Traffic Flows – VPC Internal communication



No NAT

- By default, traffic between VPC subnets of any type part of the same VPC flows directly without Network Address Translation.
- This subnet-to-subnet routing occurs through the VPC's implicit router, which directs traffic between different subnet networks.

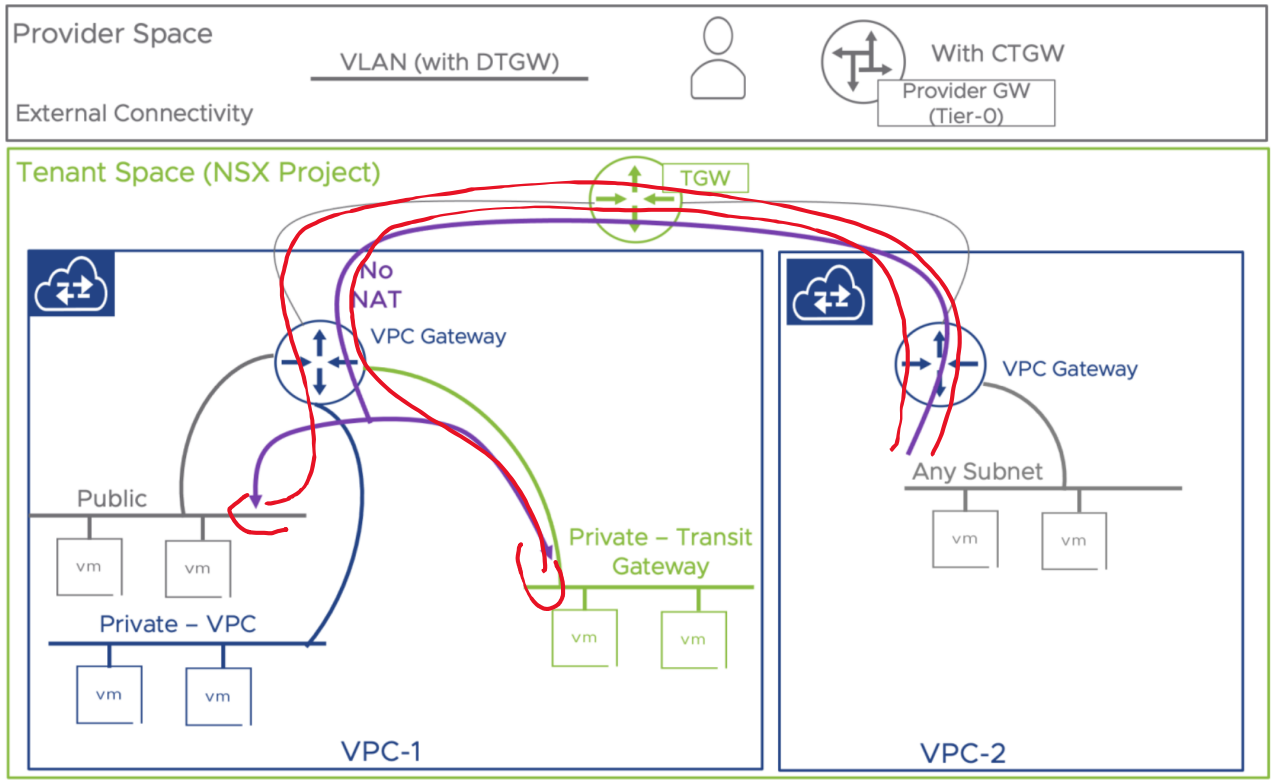
Traffic Flows – VPC Internal communication (Ext IP)



NAT via External IP

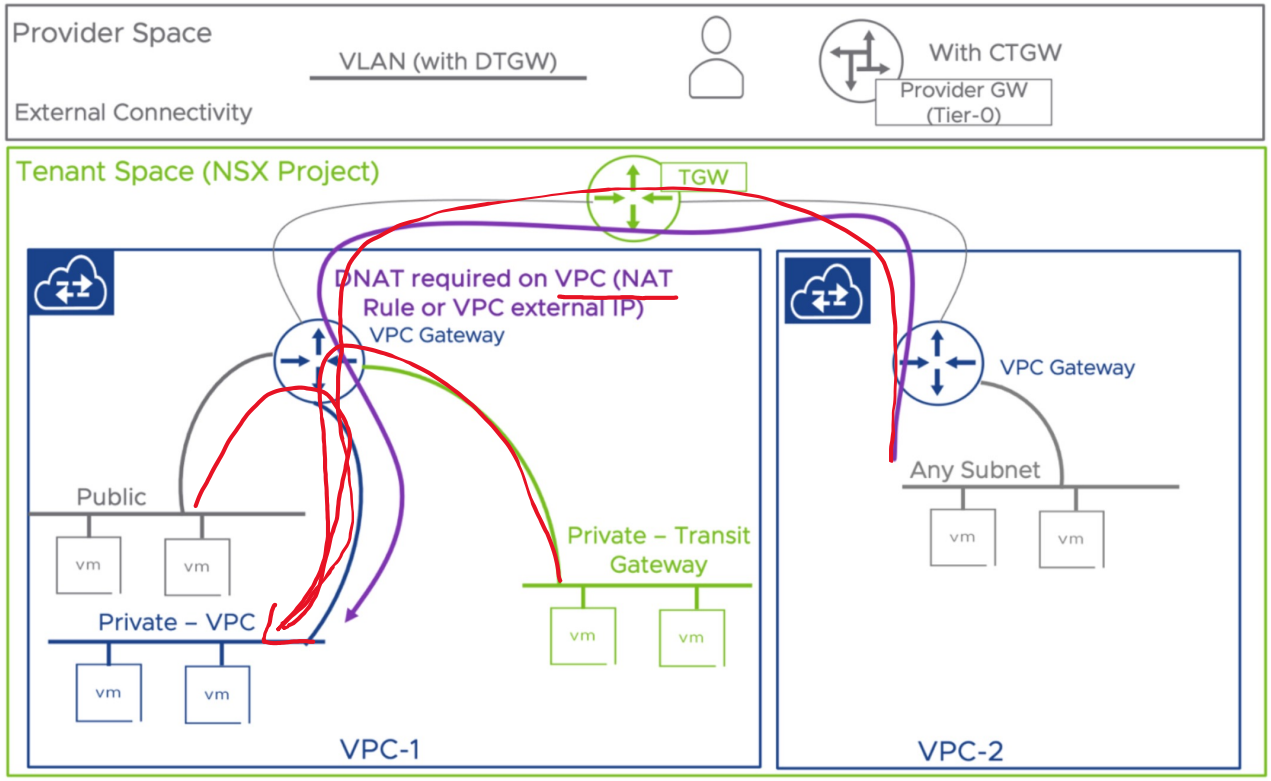
- External IPs are implemented as paired DNAT/SNAT rules on the VPC Service Router (SR) when using CTGW or DTGW.
- In CTGW setups, internal-to-external communication within the same VPC requires SNAT to ensure proper return path via the SR for reverse translation.
- DTGW, internal VPC traffic to External IPs is not supported

Traffic Flows - Inter-VPC communication (Same TGW)



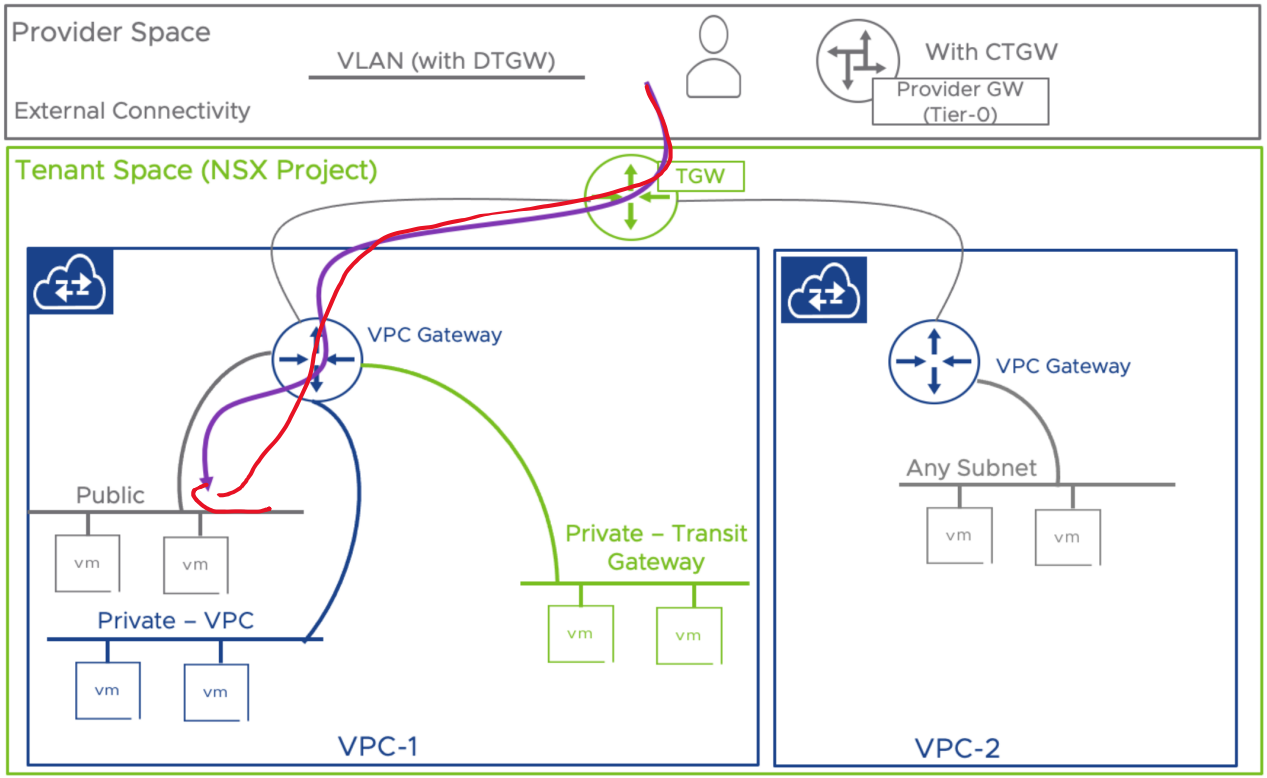
- Public and Private-TGW subnets support direct routing between VPCs via the TGW – no DNAT required.
- Native IPs are preserved, simplifying communication across VPCs connected to the same TGW.
- Private VPC subnets cannot be reached via inter-VPC communication.

Traffic Flows - Any subnet to Private-VPC Subnet



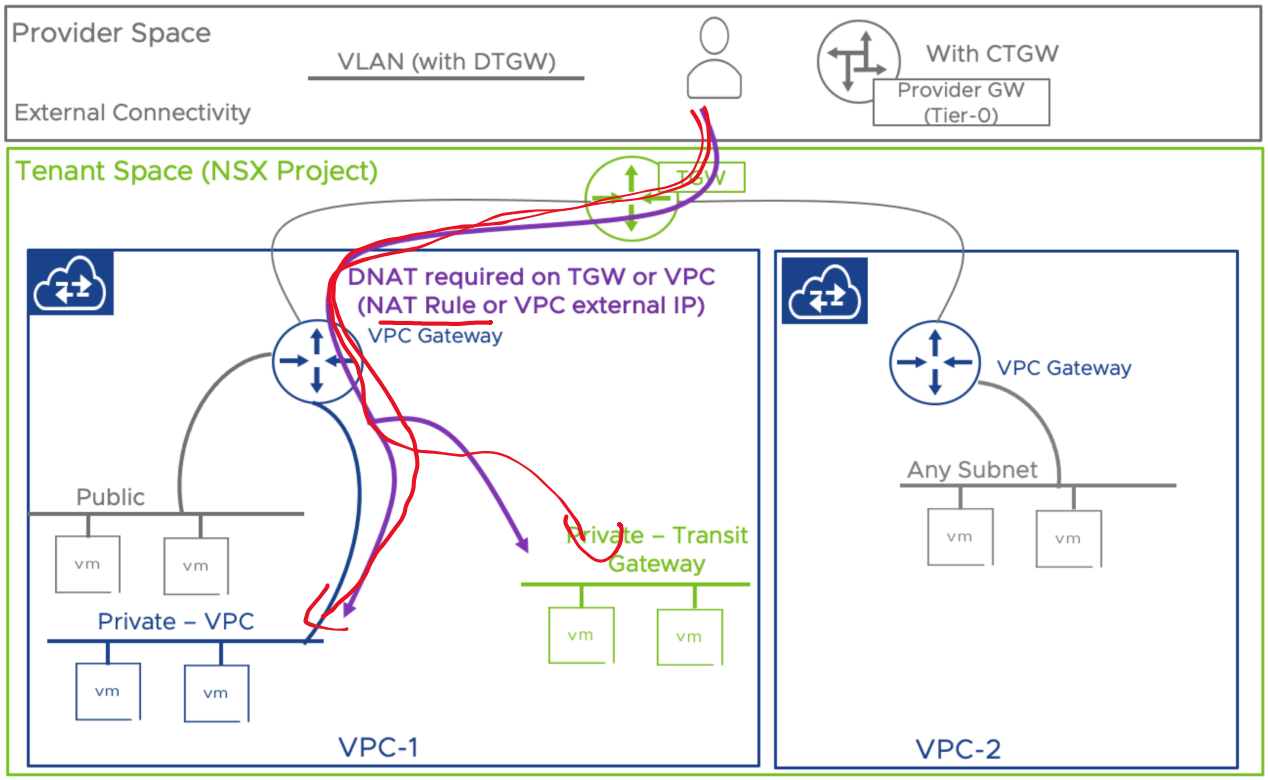
- DNAT is required when targeting workloads on private-VPC subnets across VPC boundaries.
- DNAT can be implemented via a static DNAT rule, reflexive NAT
- All options require north-south services to be enabled on the VPC gateway, preserving routing and security isolation.

Traffic Flows - VPC Inbound Communication



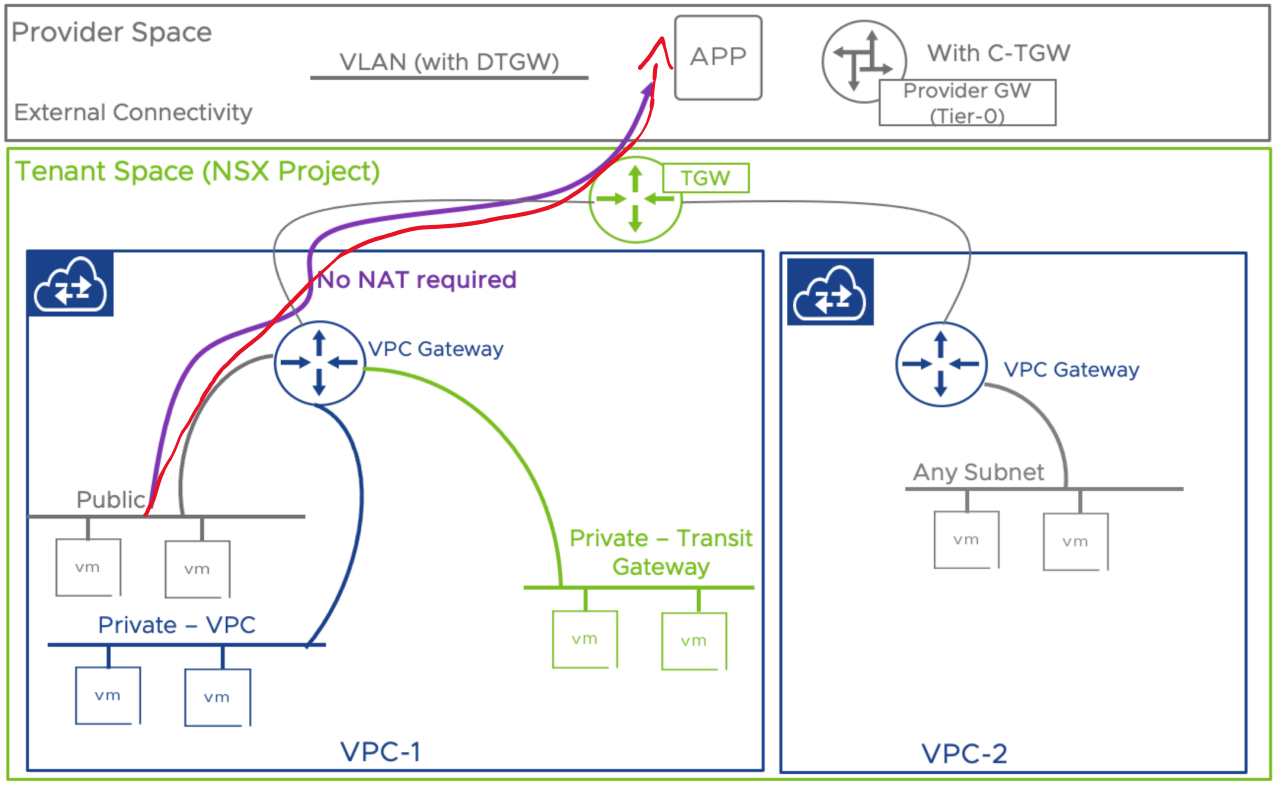
- No DNAT is required for traffic from external clients to workloads on public subnets.
- Public subnets are natively routable and designed for direct external accessibility.

Traffic Flows - External Access to Private Subnets



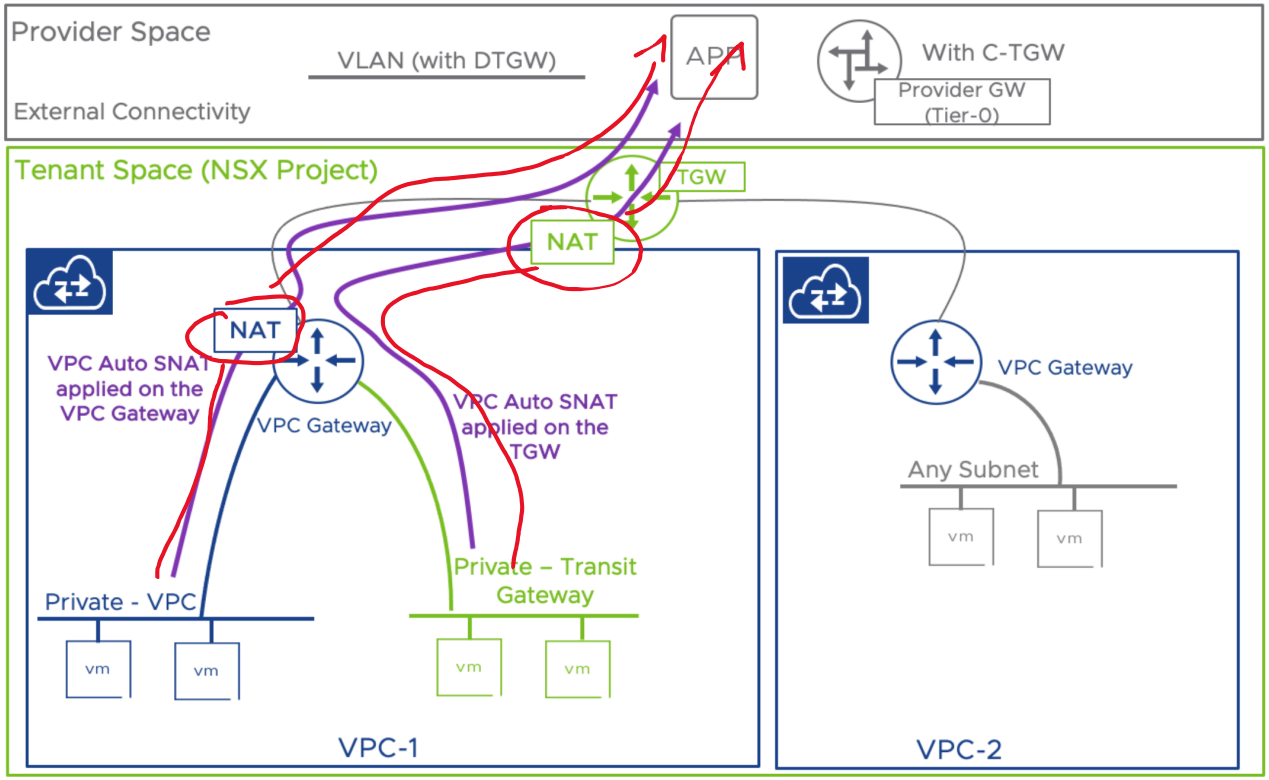
- DNAT is required for external access to private-VPC and private-TGW subnets.
- DNAT can be applied via VPC gateway (static or reflexive NAT) or by assigning an External IP to the workload.
- DNAT at the Transit Gateway
  - Active/Standby mode for DNAT
  - Reflexive NAT works in Active/Active, Active/Standby mode or distributed

Traffic Flows - Outbound Traffic from Public Subnets



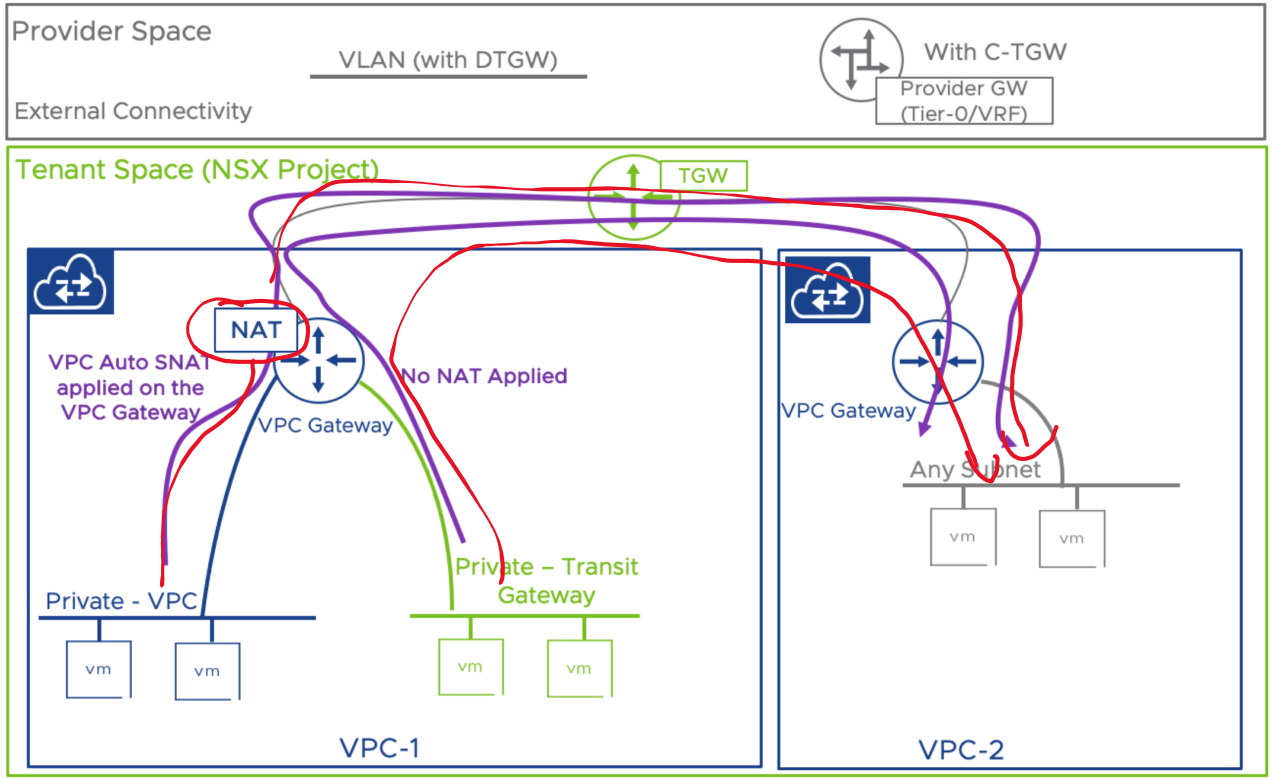
- No SNAT is required when workloads on public subnets communicate with external endpoints.
- The original source IP is preserved end-to-end, enabling direct response from external systems.
- Simplifies outbound connectivity and supports IP visibility for auditing or security use cases.

Traffic Flows - Outbound Traffic with Auto-SNAT



- Private-VPC and Private-TGW subnets use Auto-SNAT for outbound traffic to external endpoints, unless overridden by higher-priority rules.
- SNAT rules are applied on the VPC Gateway (for Private-VPC) and on the Transit Gateway (for Private-TGW; requires Active/Standby mode).
- To avoid port conflicts, the system performs Port Address Translation (PAT) using non-overlapping port ranges.

Traffic Flows - Outbound Traffic to other VPC



- Private-VPC subnets use Auto-SNAT on the VPC Gateway when sending traffic to other VPCs connected to the same TGW.
- The source IP is translated, enabling controlled and isolated cross-VPC communication.
- Private-TGW subnets do not require SNAT and retain their original source IP during inter-VPC traffic.

Brief summary (not all cases)

Subnet Type	Outbound to External	Inbound from External
Public	No NAT	No NAT
Private-TGW	SNAT	DNAT required
Private-VPC	SNAT	DNAT required

Subnet Type	Public other VPC	Private-TGW other VPC	Private-VPC other VPC
Public	No NAT	No NAT	DNAT at target
Private-TGW	No NAT	No NAT	DNAT at target
Private-VPC	SNAT required	SNAT required	SNAT at source + DNAT at target

Thank you!

Daniel Krieger

evoila

Your Feedback Is Important

Please take a minute to complete the survey session in the mobile app.

1. Navigate to this session
2. Take this survey
3. Enjoy your next session!


VMUG
CONNECT
Progress Powered by Community