

Seamless Connections Elevating VCF Networking

Mujtaba Mir
Principal Solutions Engineer

September 2026



A stylized illustration of a coastal scene. In the foreground, there's a dark blue silhouette of a coastline with a few buildings. The middle ground shows a blue body of water with several white sailboats. In the background, a large yellow sun is partially obscured by a multi-colored rainbow (yellow, orange, red, purple) that arches across the sky. Three stylized birds are flying in the sky above the rainbow.

Agenda

- Network Virtualization
- NSX Components
- Virtual Private Cloud (VPC)
- What's New?

Network Virtualization



Network Virtualization is Required to Deliver a Modern Private Cloud

Network Virtualization



Integrated SDN

Self-service networks with Virtual Private Cloud

Virtual distributed switching & routing

Consistent networking policies across sites

Modern Apps Networking



Simplified K8s Networking

Comprehensive network policy model

K8s platform agnostic

Integration with NSX offers a single pane of glass

Network Visibility and Troubleshooting



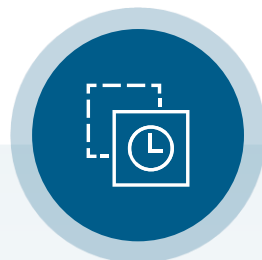
Powerful Monitoring

Pre-deployment assessment

Application discovery

Network topology and metrics visualization

Workload Mobility



Large-scale Mobility

Any-to-any vSphere version

Zero-downtime migration

Various migration modes

Lateral Security*



E-W Traffic Protection

Stateful L7 Distributed FW

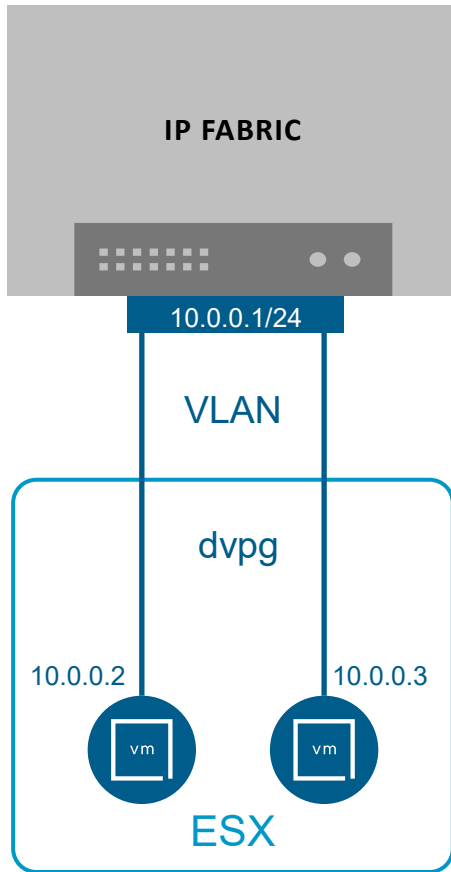
ATP with IDS/IPS, Network Sandbox, NTA/NDR

Security analytics and rule recommendations

*Add-on advanced services not included with VCF

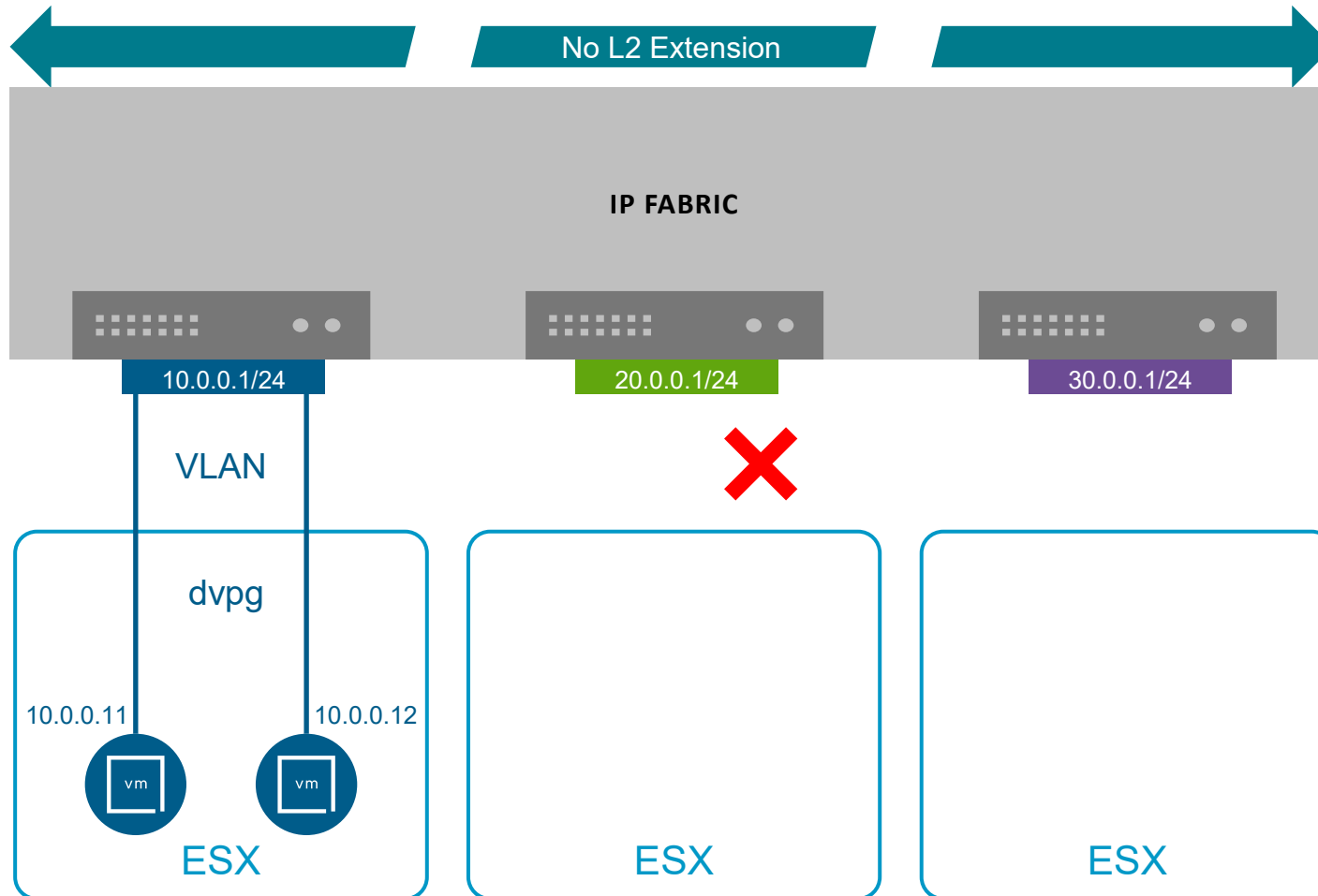
VM Running on ESX Host

The VM is virtual, the network is physical



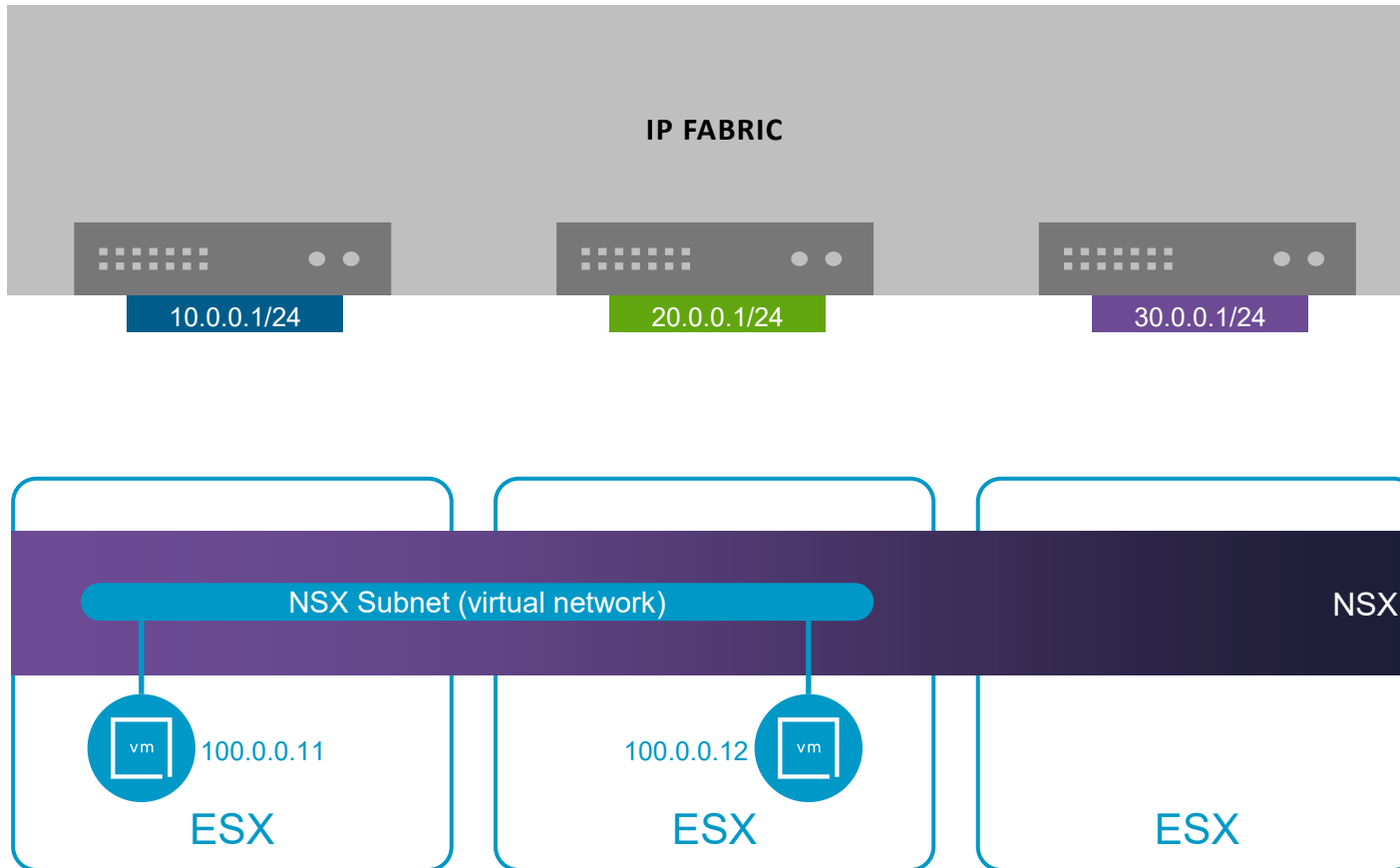
VM Mobility: a Critical Aspect of Virtualization

Current Network Design: L3 between Racks



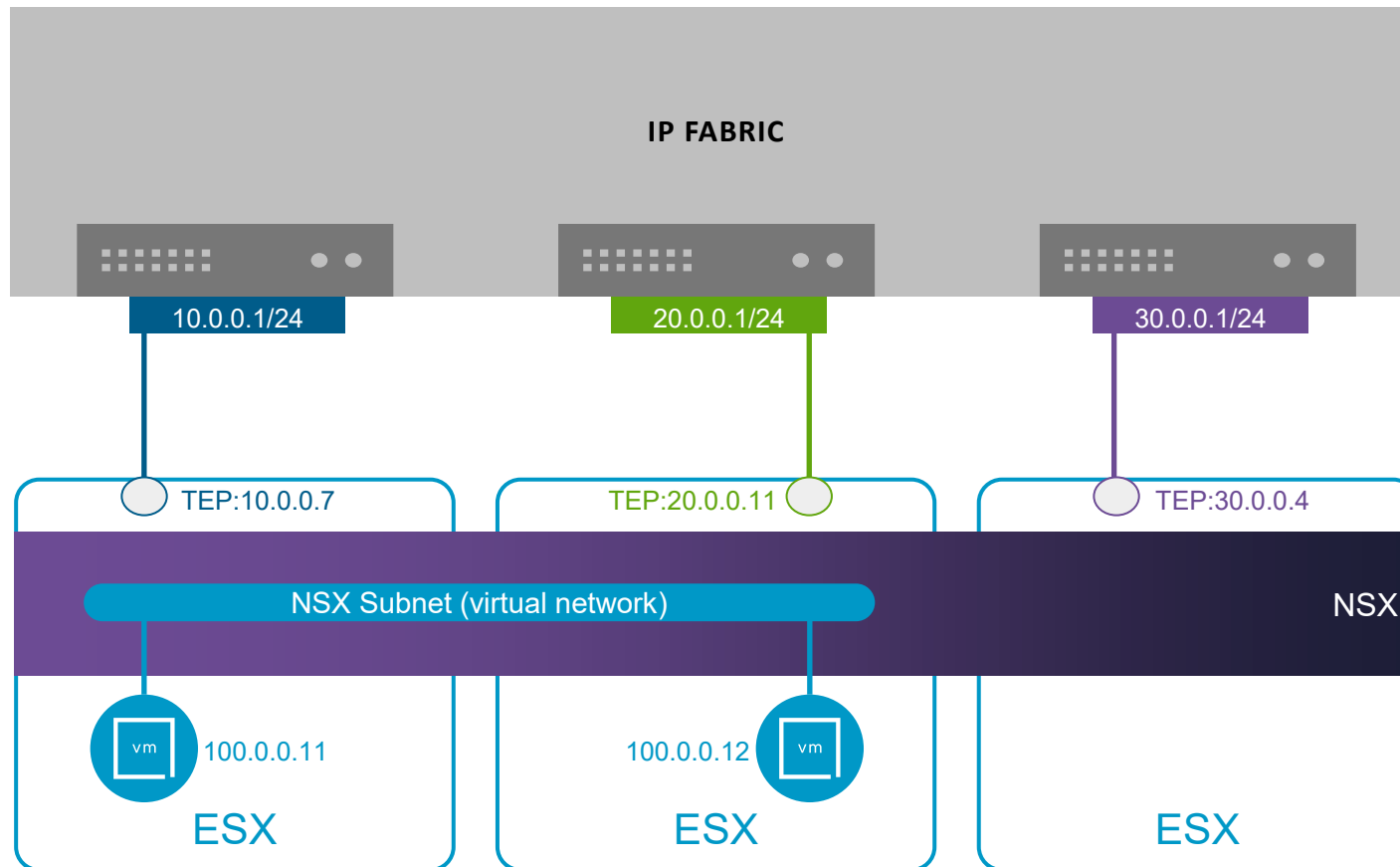
With VCF, NSX is Included and Deployed on ESX hosts

NSX enables virtual networking

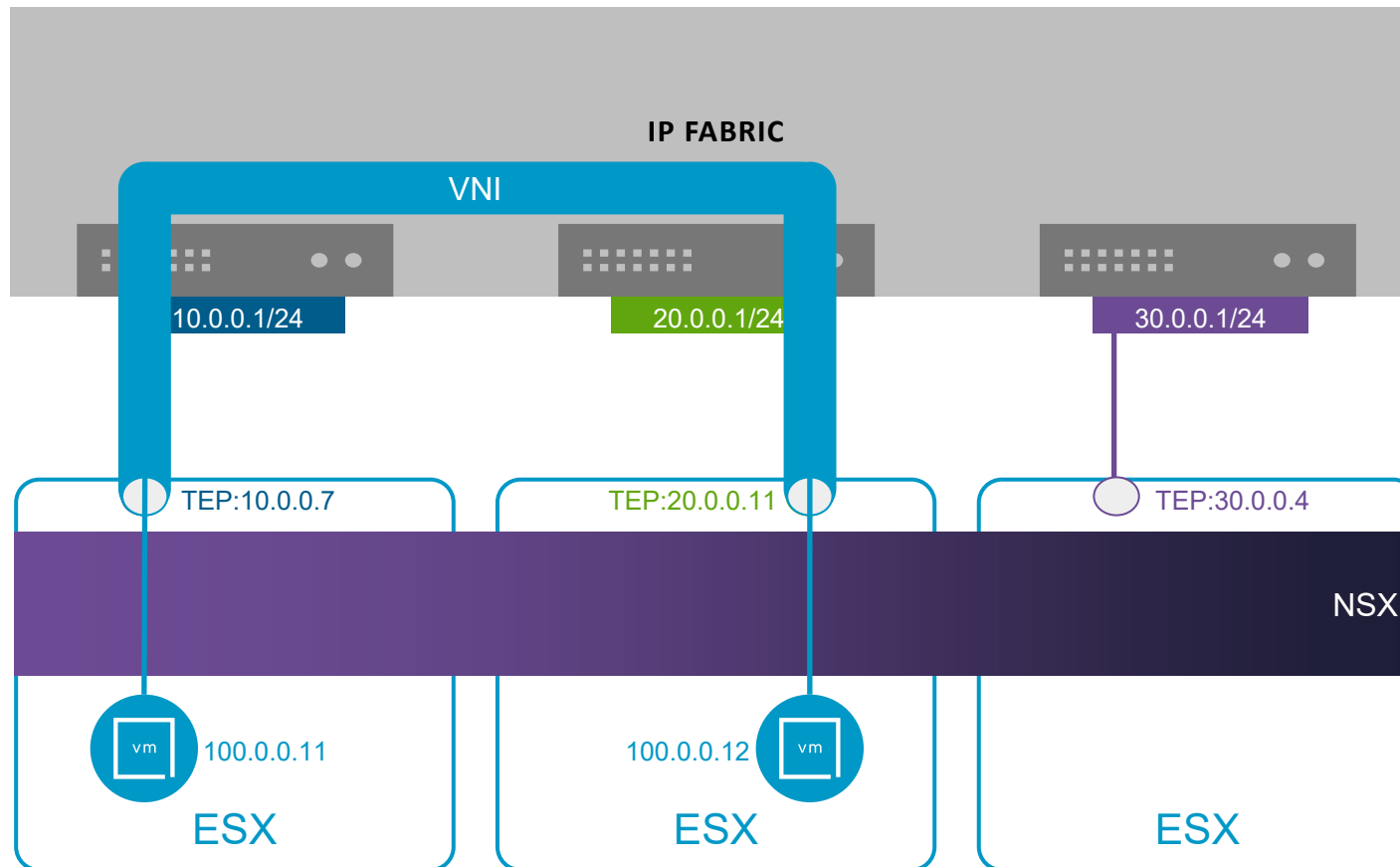


How Does Virtual Networking Work?

During VCF deployment, Tunnel End Points (TEPs) are configured

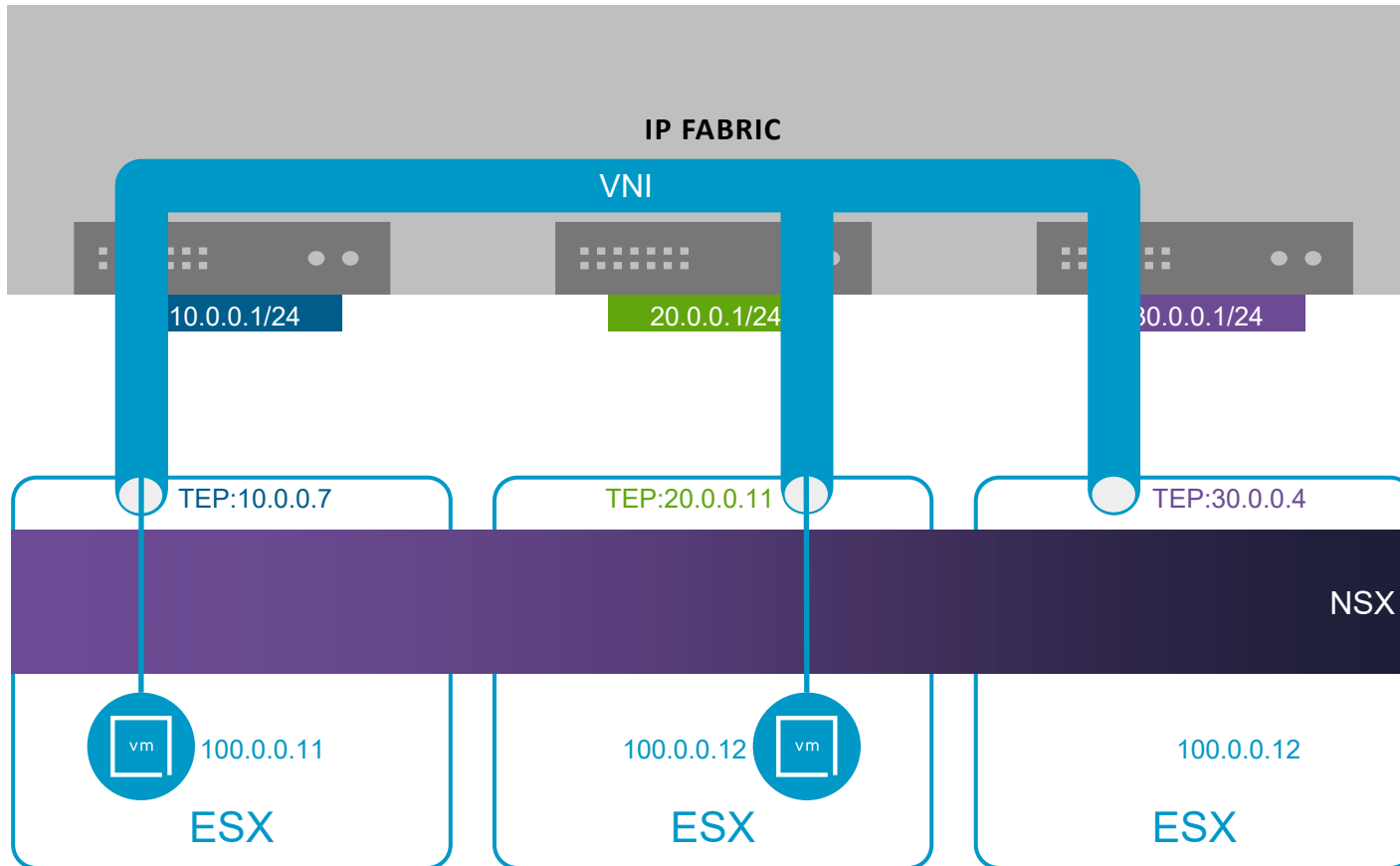


Traffic is Tunneled Between TEPs

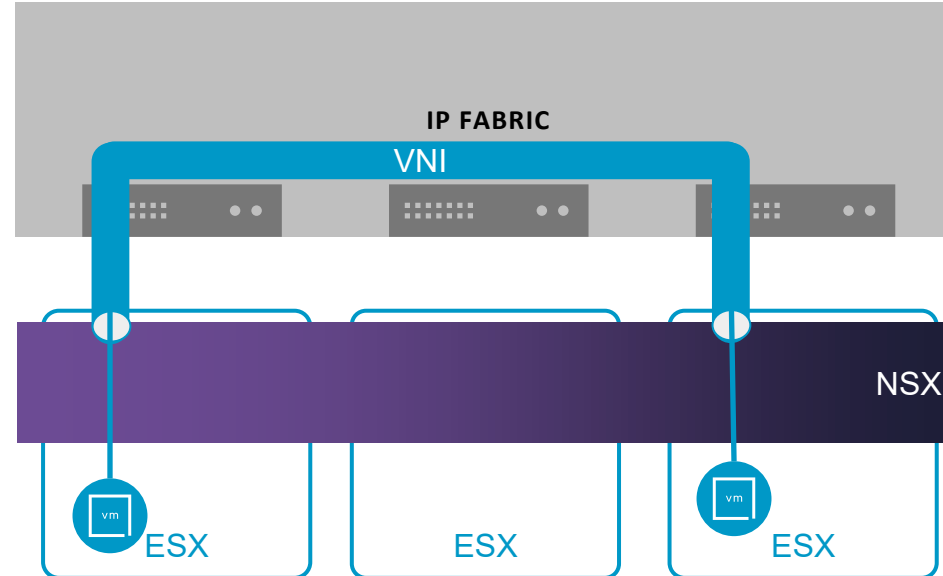


VNI: Virtual Network Identifier
(like a VLAN ID for tunnels)

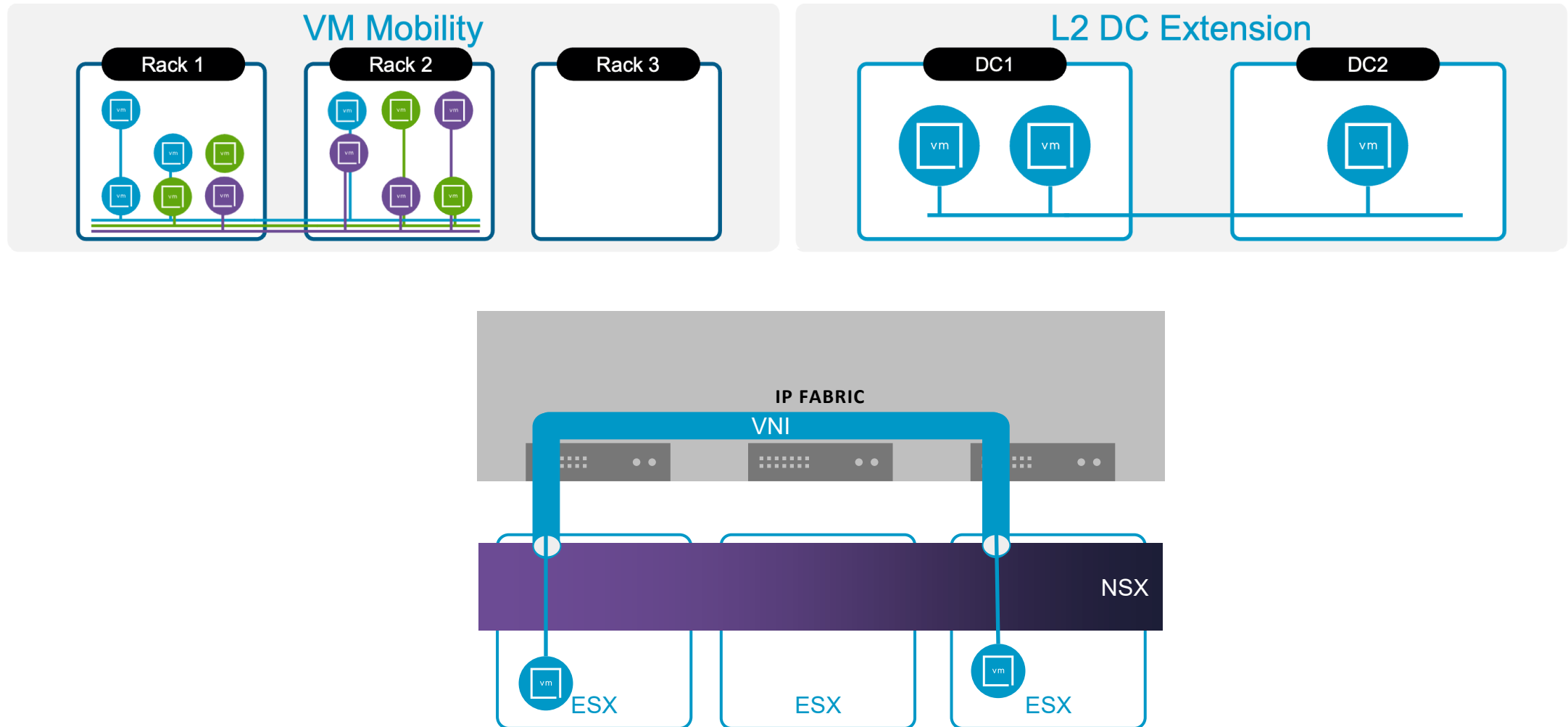
NSX Maintains Those Tunnels



VCF with NSX Virtual Networking Use Cases



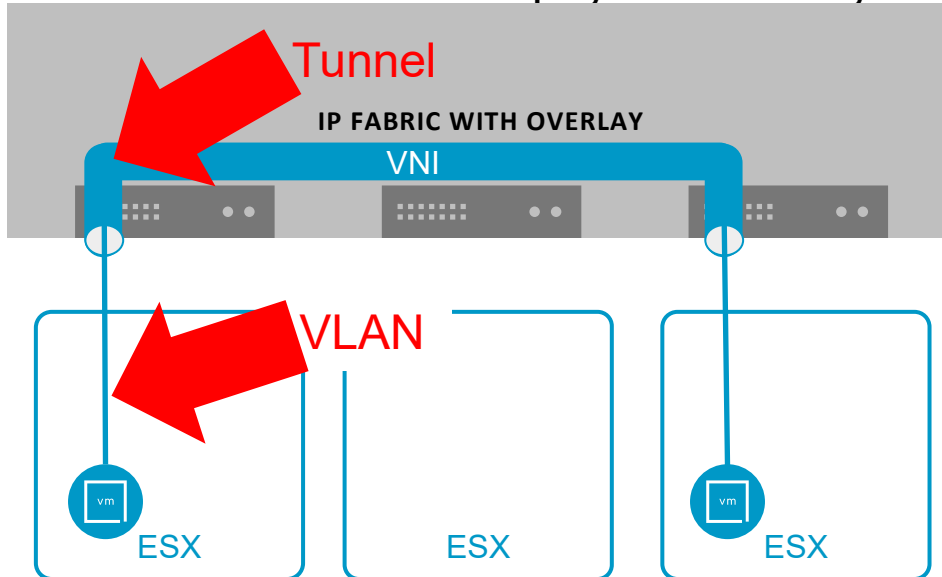
VCF with NSX Virtual Networking Use Cases



VCF with Physical Overlay vs. NSX Virtual Networking

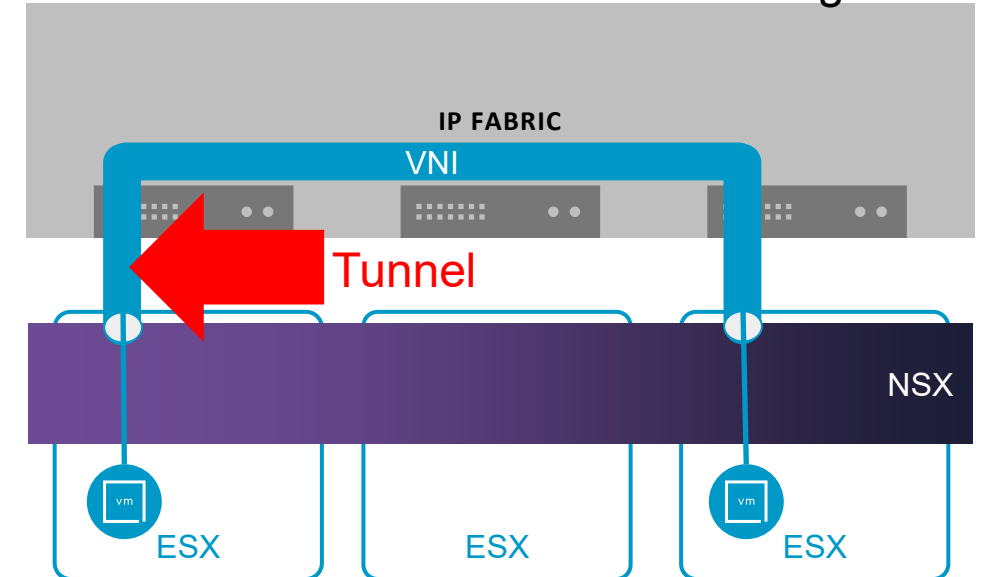
So, what's the difference?

VCF with VLAN and physical overlay



VS.

VCF with NSX virtual networking

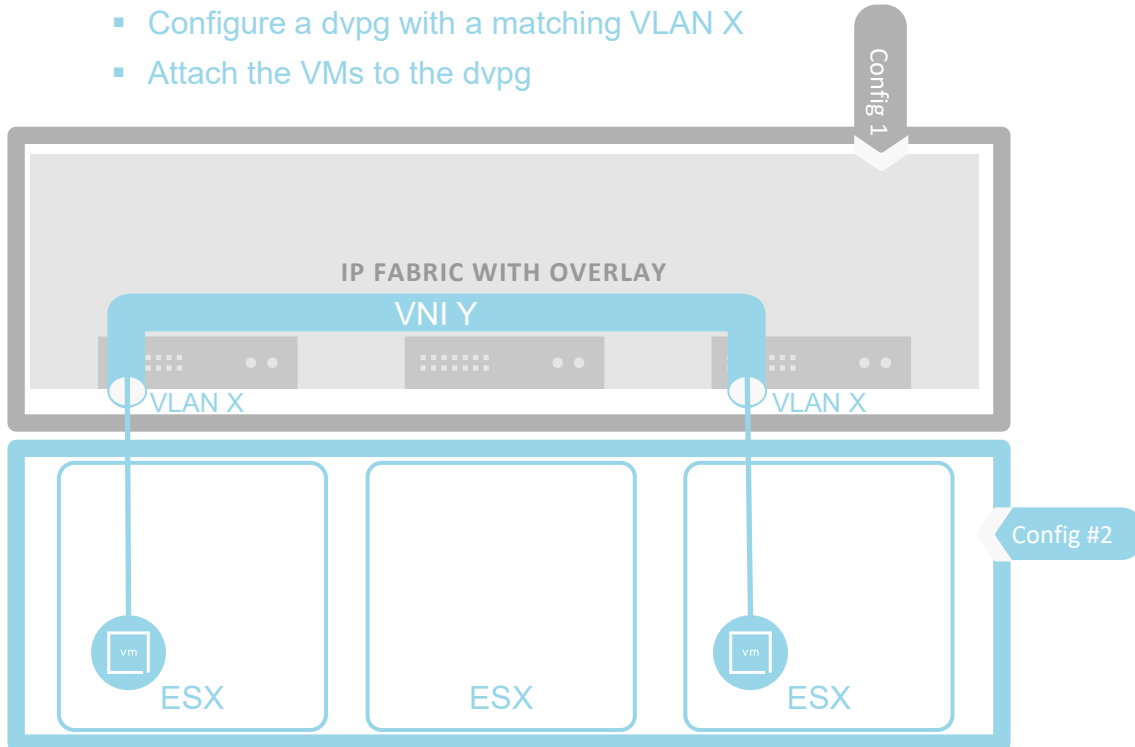


VCF with Physical Overlay vs. NSX Virtual Networking

Configuration steps

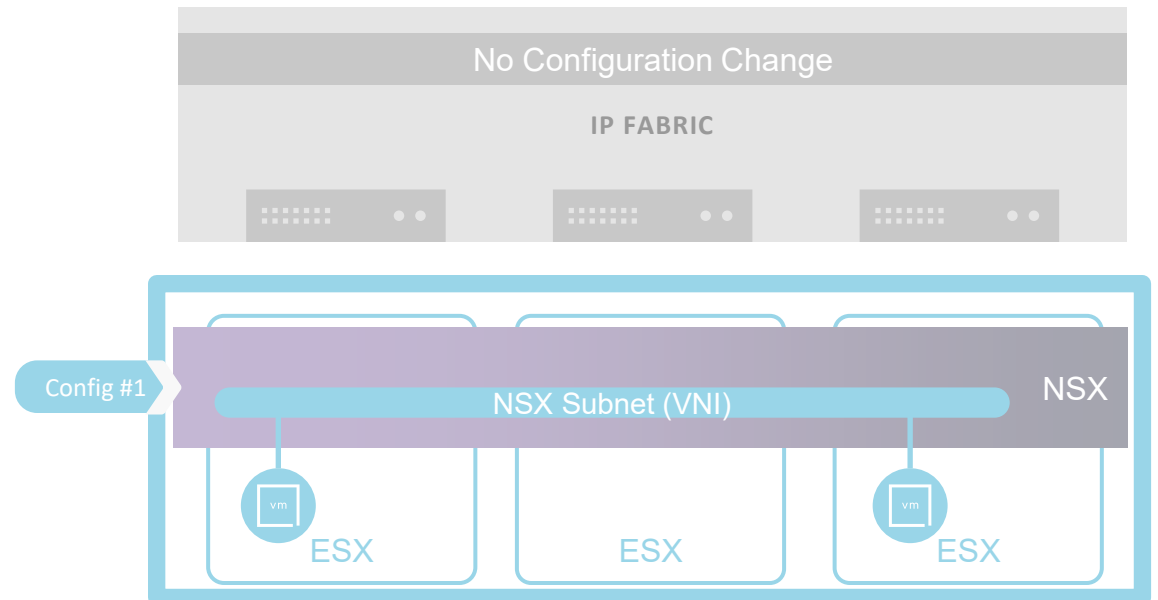
VCF with VLAN networking

- Configure a VLAN X in the physical infrastructure
- Configure a VNI Y in the physical infrastructure
- Map VLAN X to VNI Y in the physical infrastructure
- Configure a dvpg with a matching VLAN X
- Attach the VMs to the dvpg



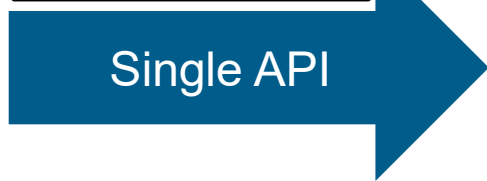
VCF with NSX virtual networking

- Configure an NSX subnet
- Attach the VMs to the subnet



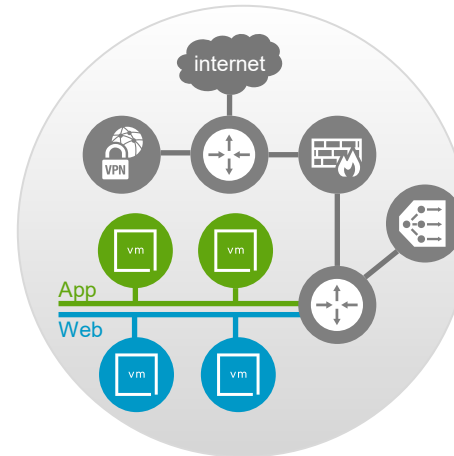
NSX builds a whole virtualized networking stack over its virtual Layer 2

NSX builds a whole virtualized networking stack over its virtual Layer 2



Deployment of a New Application in VCF

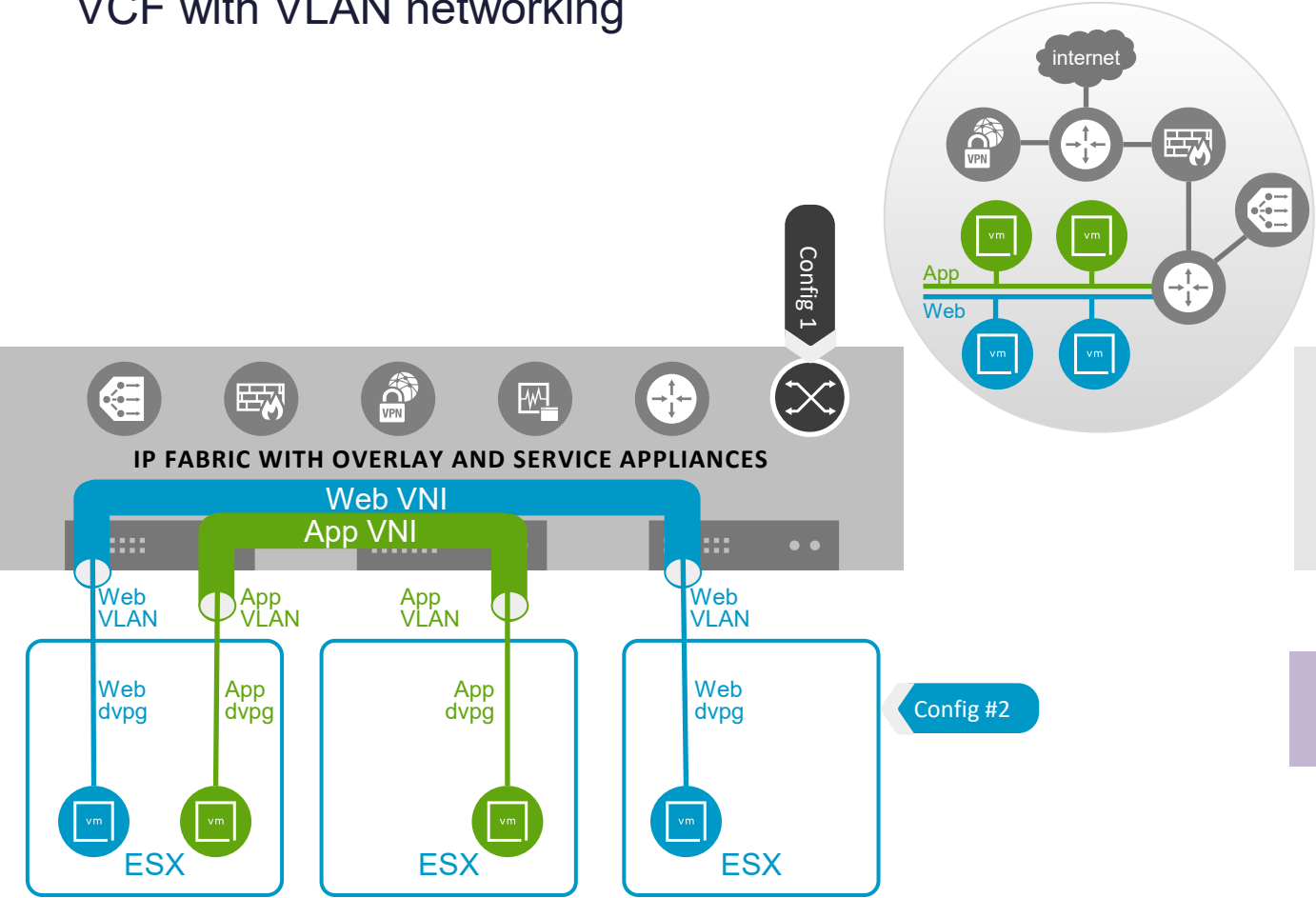
Two-tier application with services



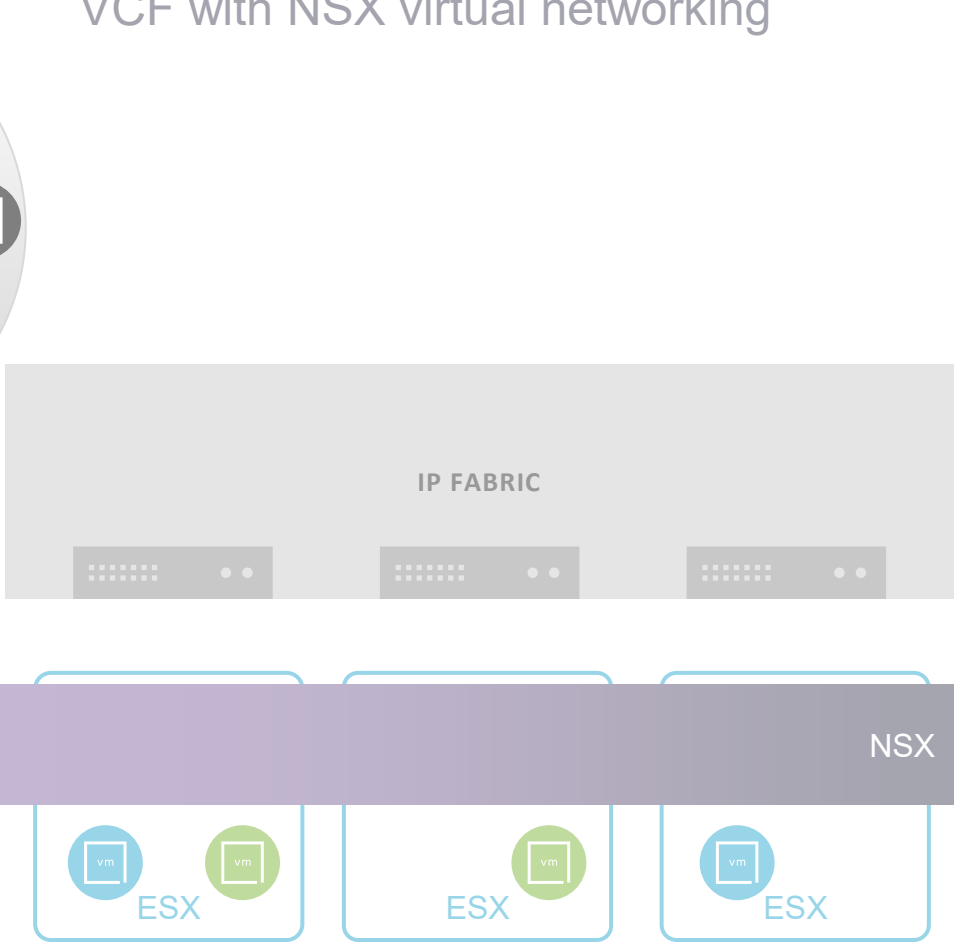
Deployment of a New Application in VCF

Two-tier application with services

VCF with VLAN networking



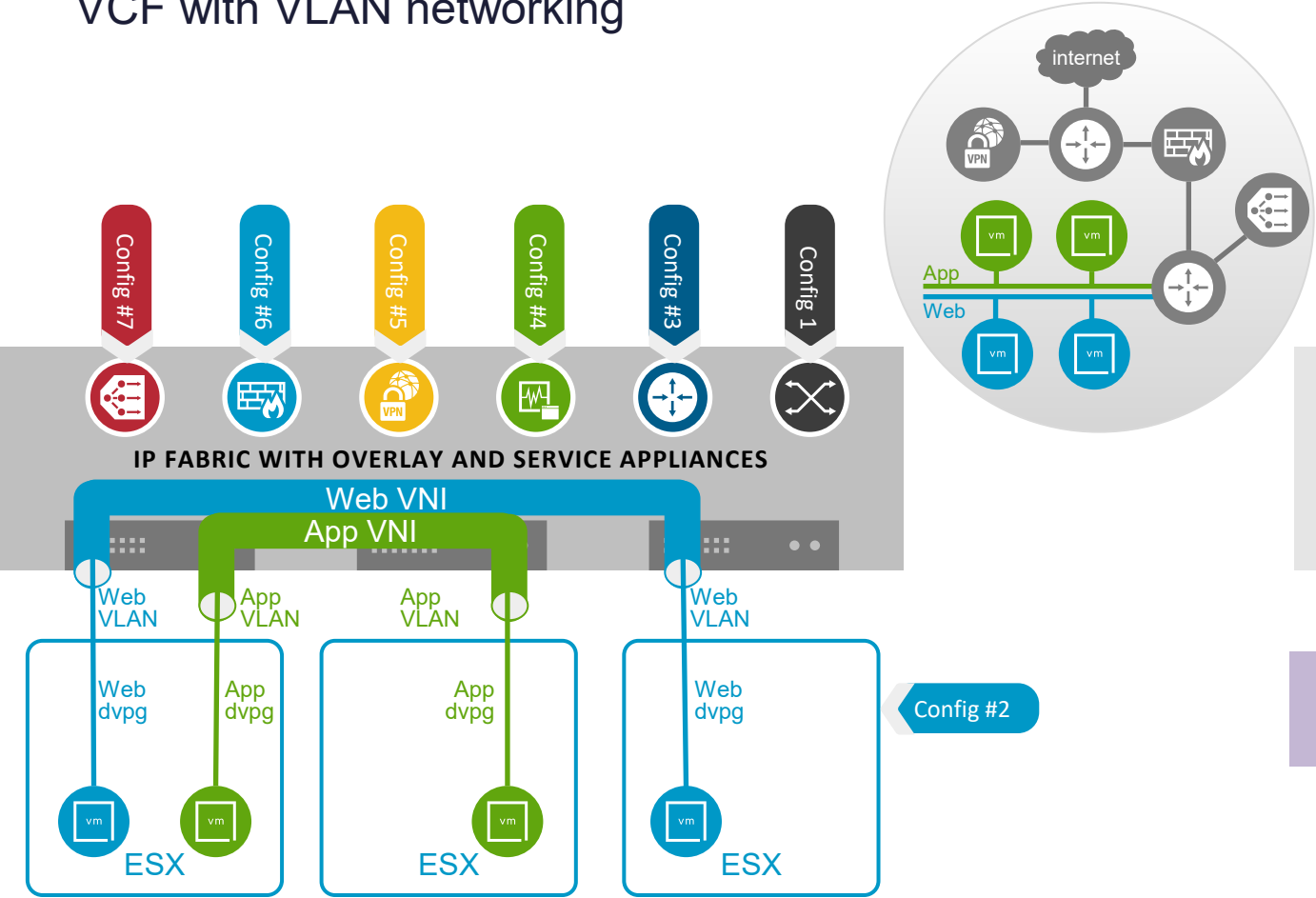
VCF with NSX virtual networking



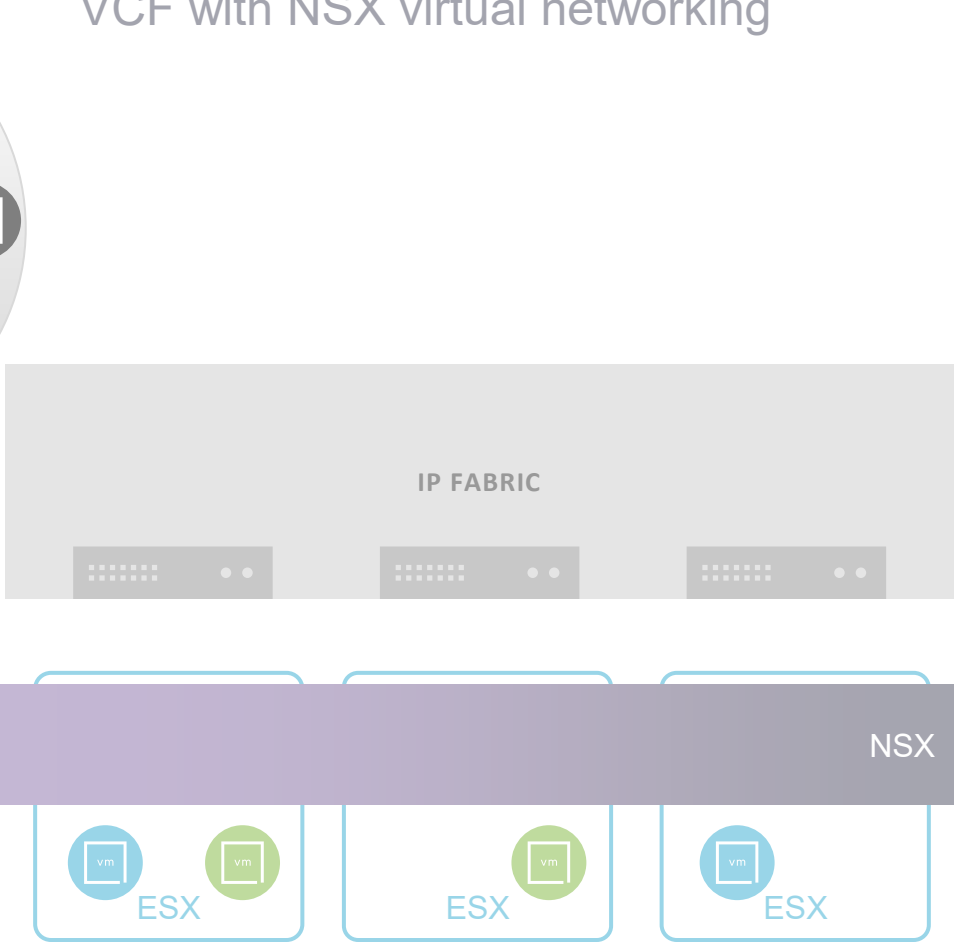
Deployment of a New Application in VCF

Two-tier application with services

VCF with VLAN networking



VCF with NSX virtual networking

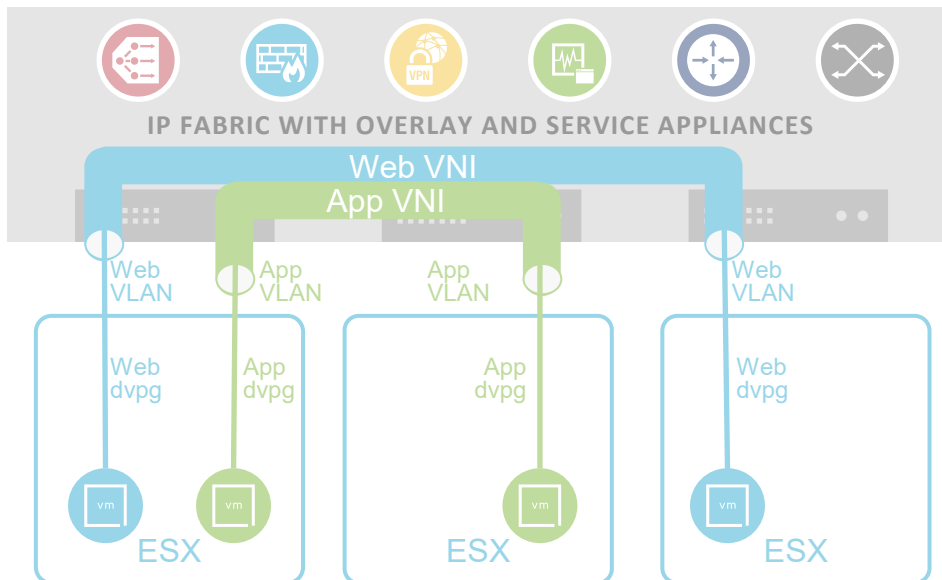
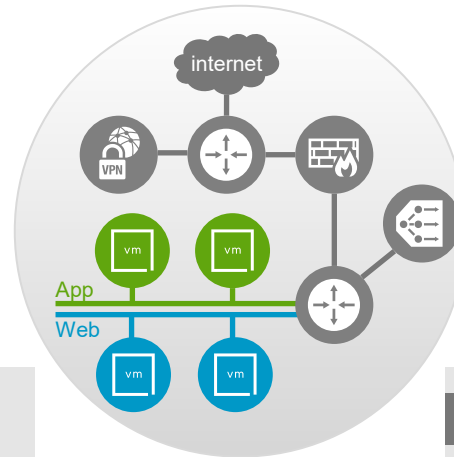


Deployment of a New Application in VCF

Two-tier application with services

VCF with VLAN networking

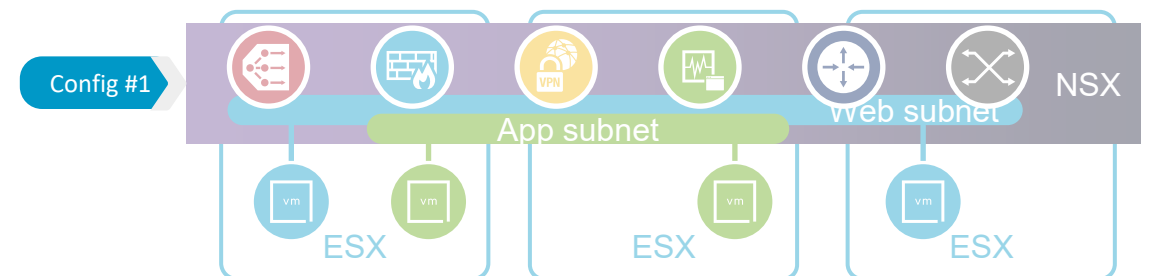
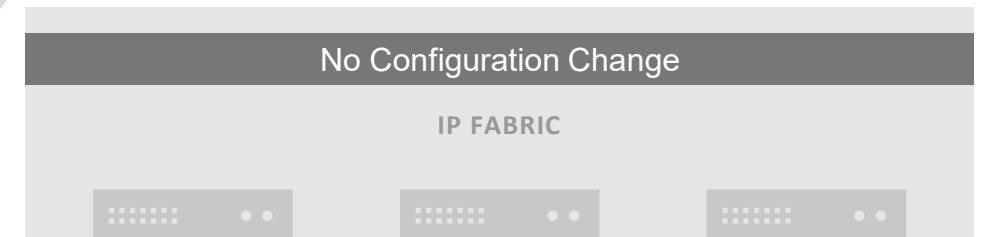
- Multiple teams involved (tickets?)
- Multiple configuration points, configuration models
- Steering traffic through appliances
- Automation is not virtualization → no elasticity



VCF with NSX virtual networking

- All network functions are virtualized
- 1 single REST API call to configure them all

This is network virtualization



Deployment of a New Application in VCF

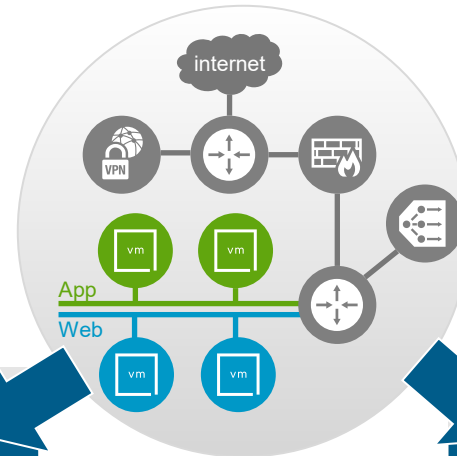
Two-tier application with services

VCF with VLAN networking

- Multiple teams involved (tickets?)
- Multiple configuration points, configuration models
- Steering traffic through appliances
- Automation is not virtualization → no elasticity

VCF with NSX virtual networking

- All network functions are virtualized
- 1 single REST API call to configure them all



This is network virtualization

Deploying a new app, can take up to:

WEEKS



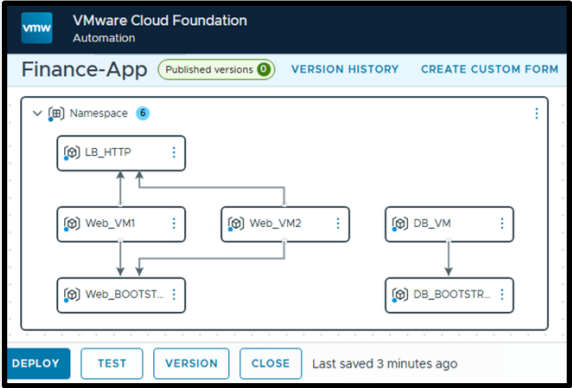
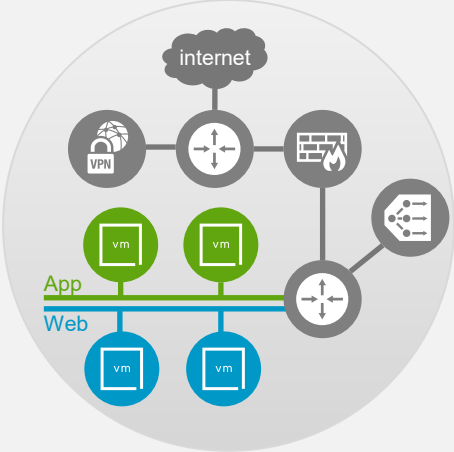
Deploying a new app, can take as little as:

SECONDS



Network Virtualization Enables

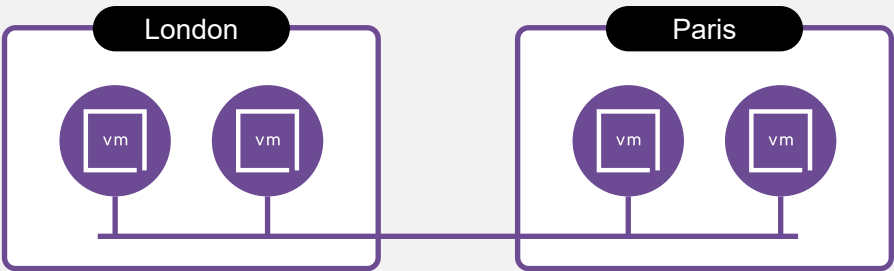
REST API
Terraform
PowerCLI
Python
...



VCF Automation



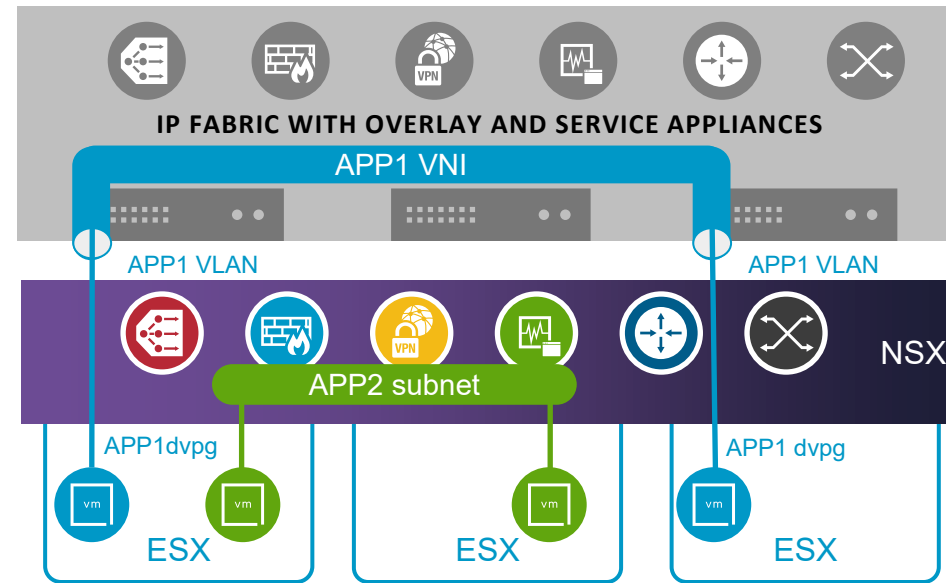
Disaster Recovery



Multi-Site

VLANs and Virtual Networks Coexist

No migration... just more options!

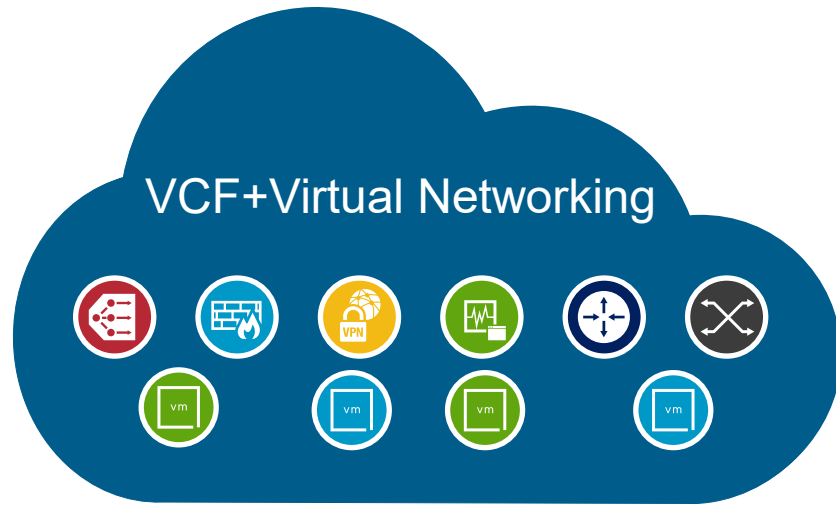


NSX virtual networking is just an added functionality

No need for migration, VLAN backed applications are unaffected by NSX

Keep deploying workloads on VLANs, and try NSX alongside them — no migration required

VCF + Virtual Networking = True Cloud-Like Experience

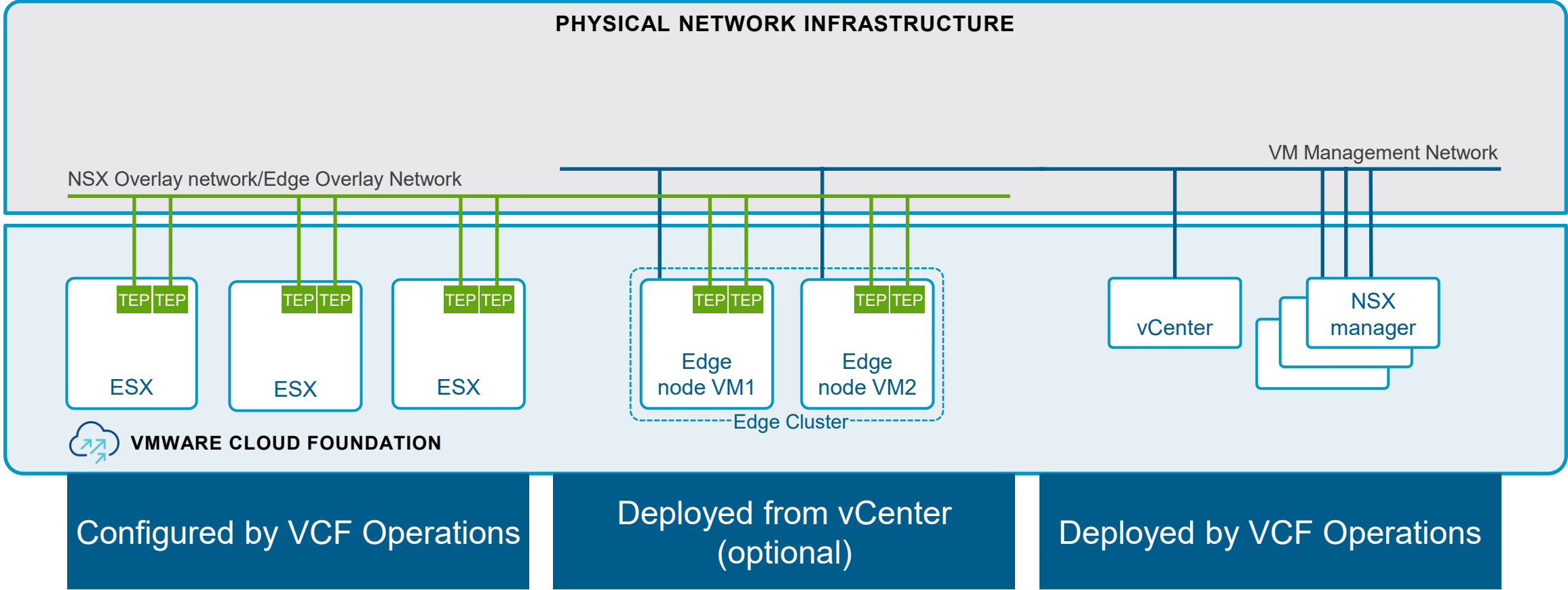


- Breaks down silos: full VM mobility across racks & sites
- Simplifies networking: no dependency on physical switch config
- Delivers full virtual stack: switching, routing, firewall, load balancing, VPN...
- Scales like the cloud: elastic, API-driven, automated
- Accelerates app deployment: weeks → seconds

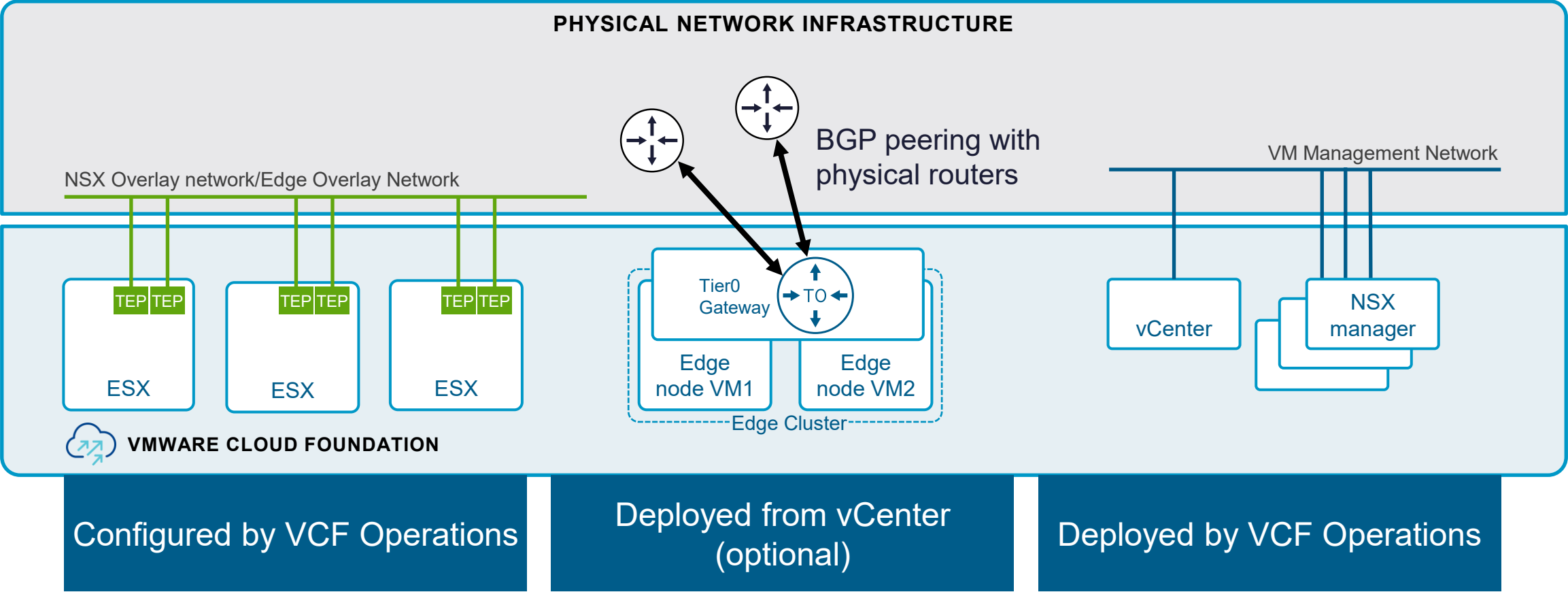
NSX Components



NSX Components



NSX Components



Deploy NSX Edges Easily

Guided edge deployment workflow available in vCenter

vSphere Client

Configure Edge Node

Edge Node Name (FQDN) *

vSphere Cluster *

Resource Pool

Host Group Affinity ☐ Yes ☒ No

Data Store *

Management IP

IP Allocation ☐ DHCP ☒ Static

Port Group *

Management IP *

Default Gateway *

Uplinks

Edge Node Uplink Mapping

Virtual Interfaces	Interfaces	Active PNICs	Standby PNICs
1	fp-eth0	vmnic0	vmnic1
2	fp-eth1	vmnic1	vmnic0

TEP VLAN *

IP Allocation (TEP) ☐ DHCP ☒ IP Pool ☐ Static IP List

IP Pool *

Size: Large

Host

vcenter-mgt-p...

Active Standby

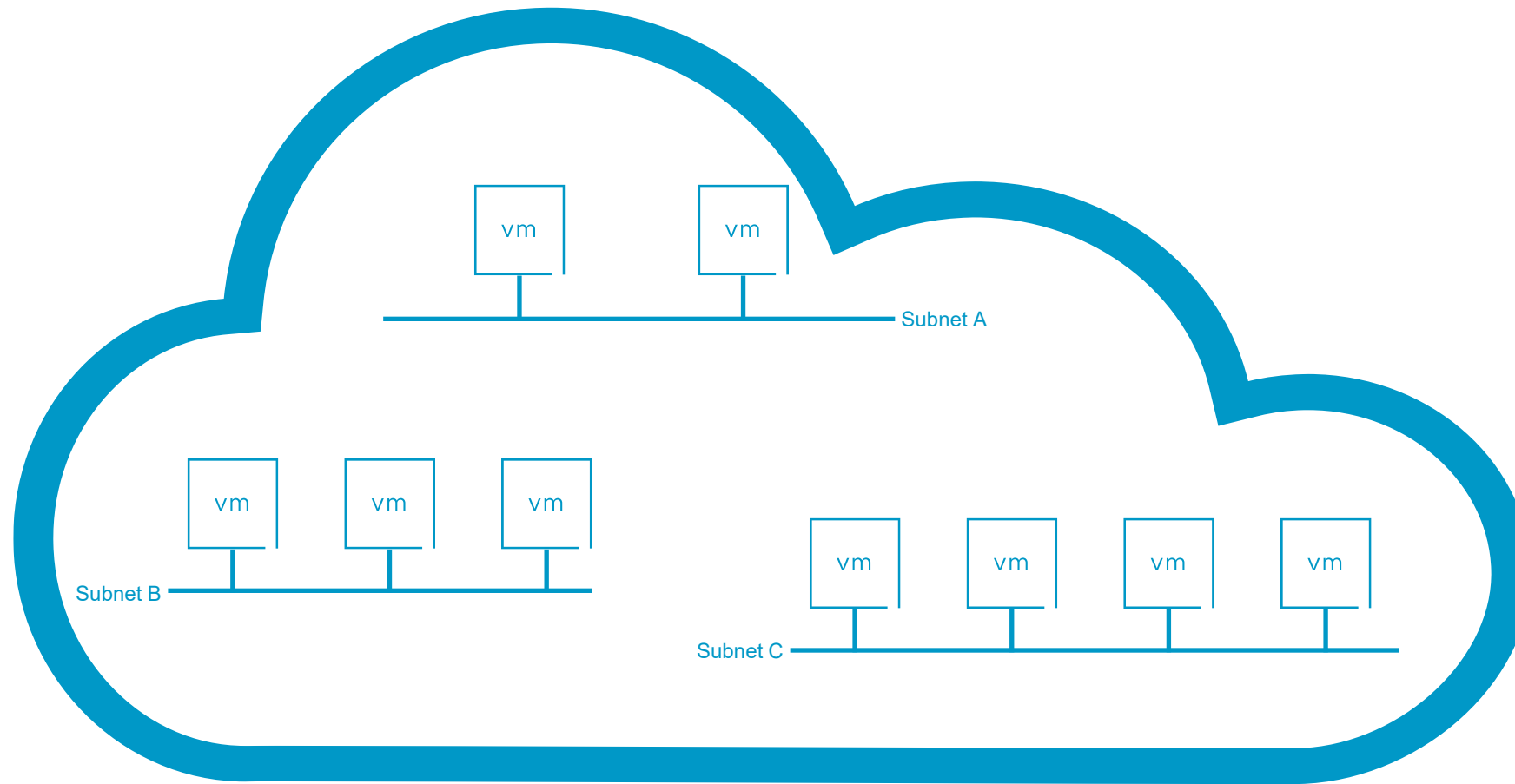
Edges are deployed with a simple vCenter UI workflow in VCF 9.0:

- the user is guided through entering the required parameters
- and a graphical representation is generated in real time

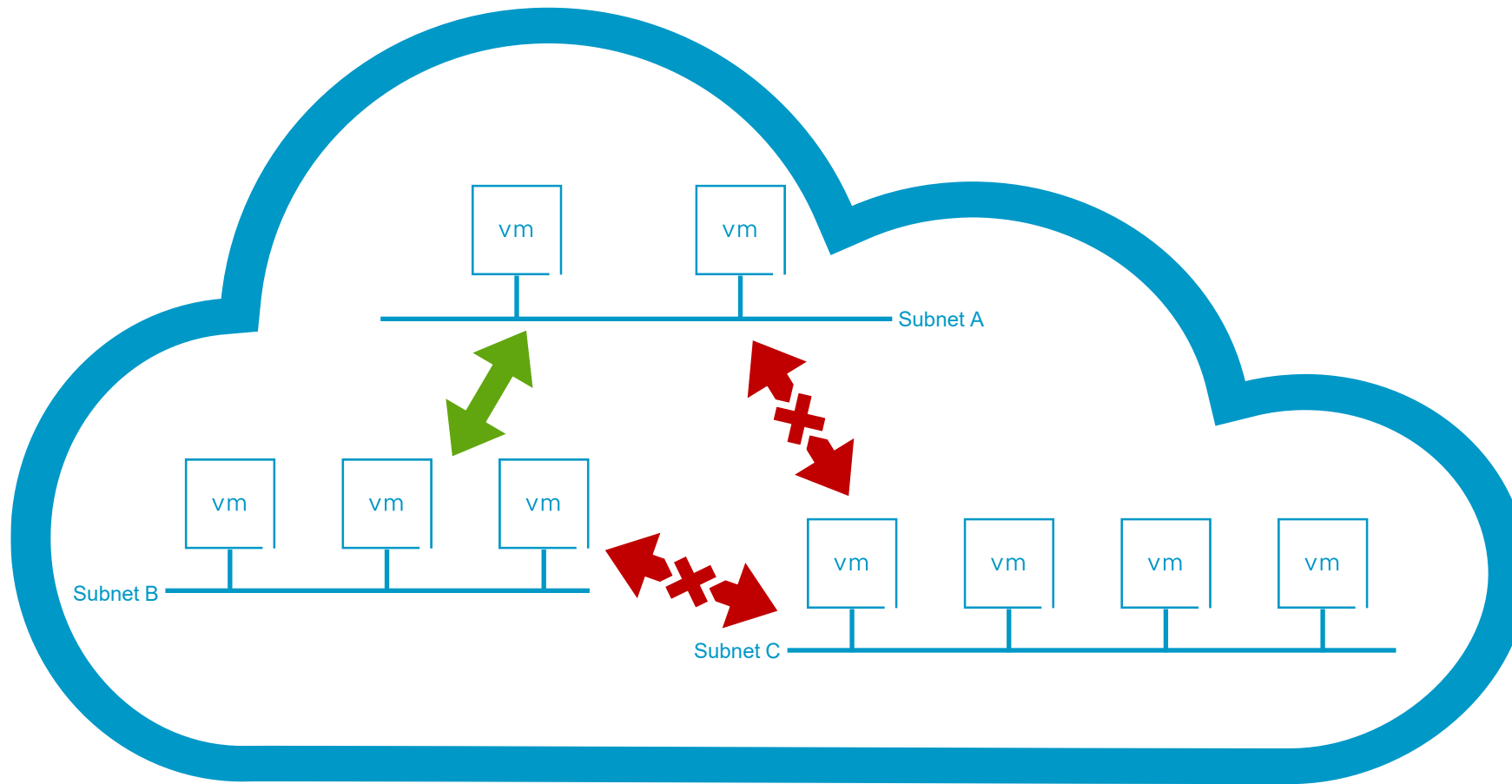
Virtual Private Cloud (VPC)



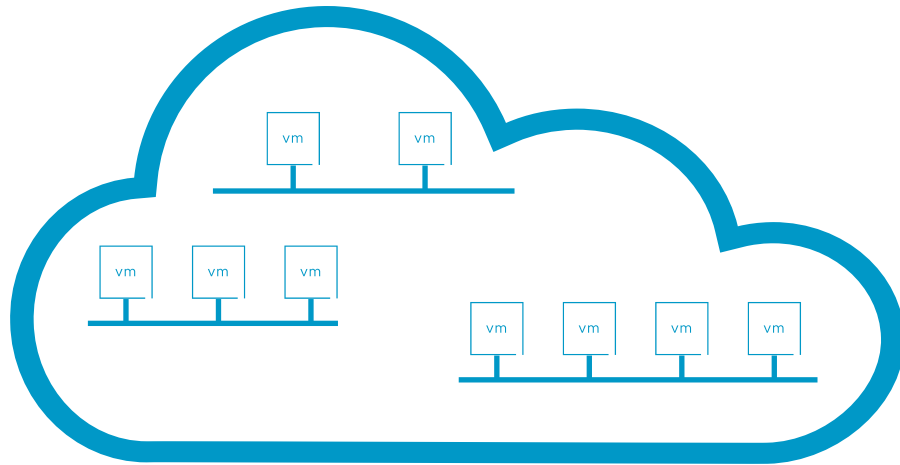
The Virtual Private Cloud (VPC)



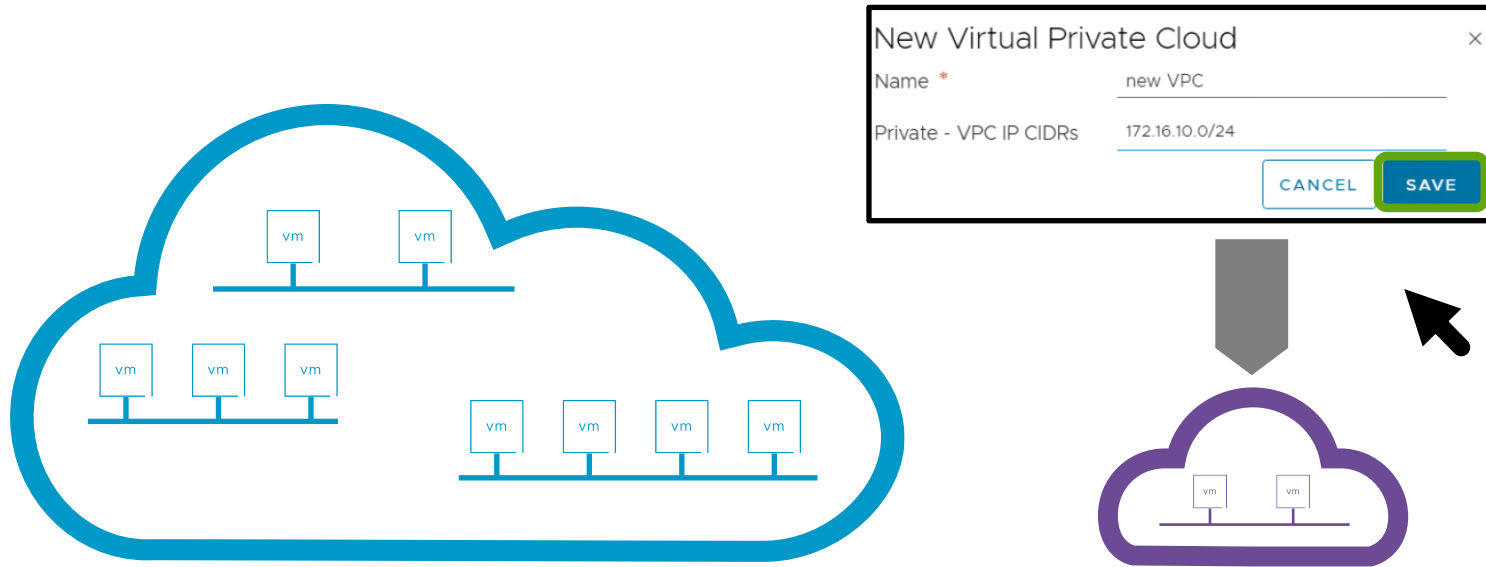
Control of connectivity within a VPC



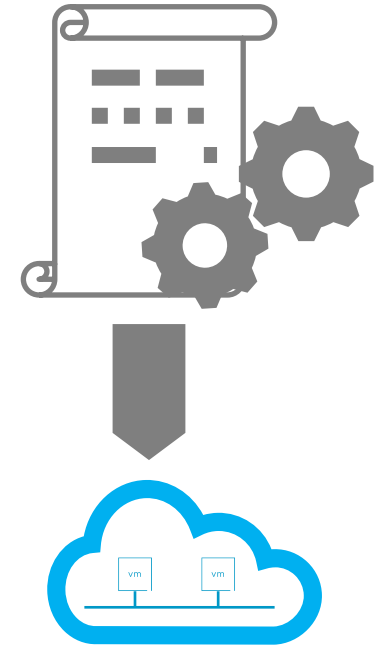
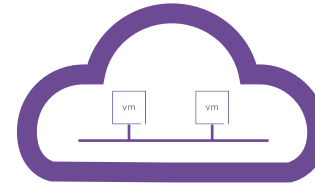
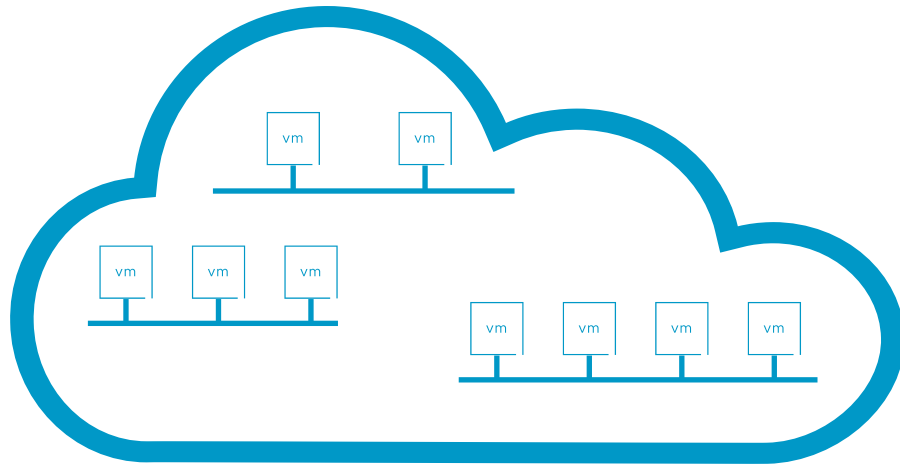
The Virtual Private Cloud (VPC)



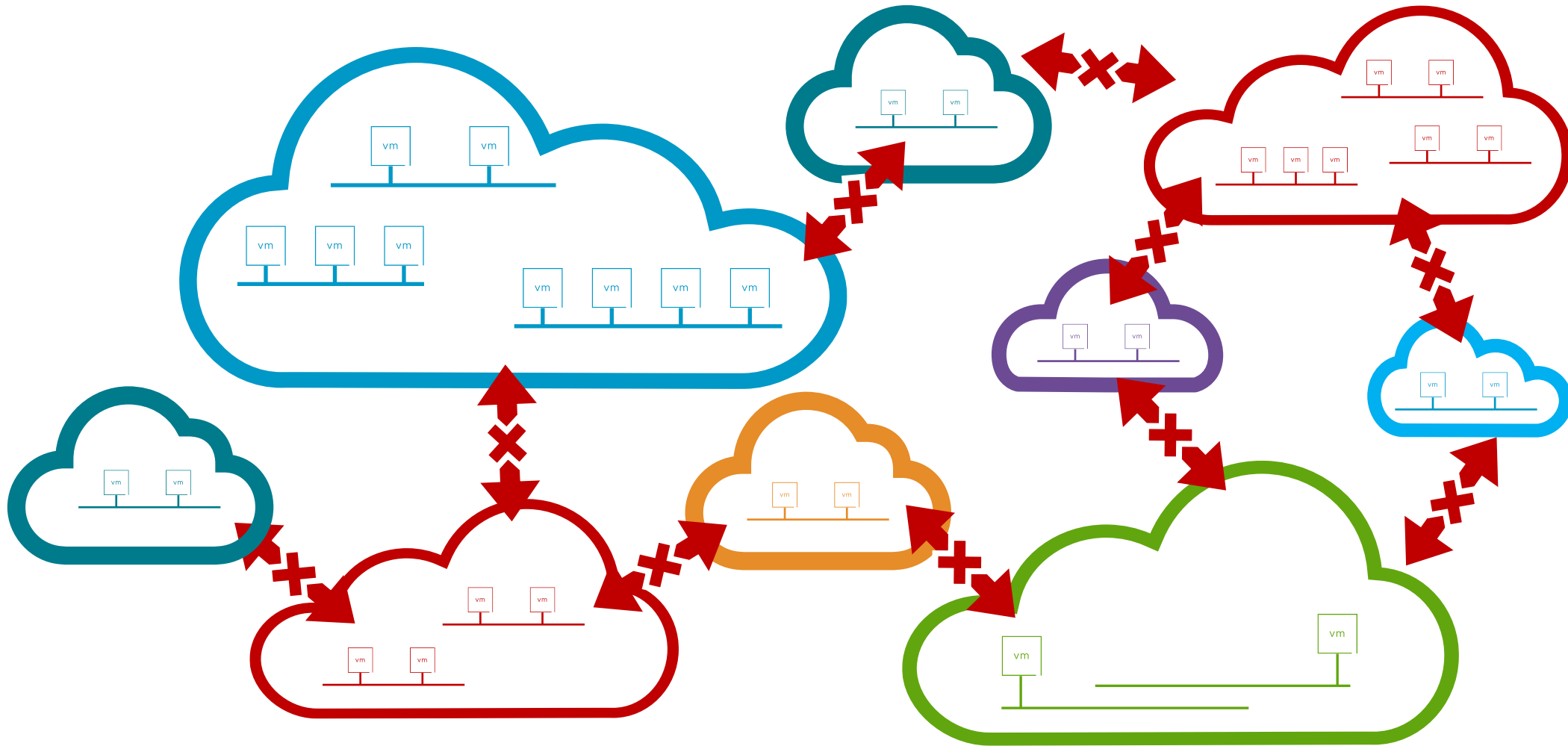
VPCs are instantly created via UI



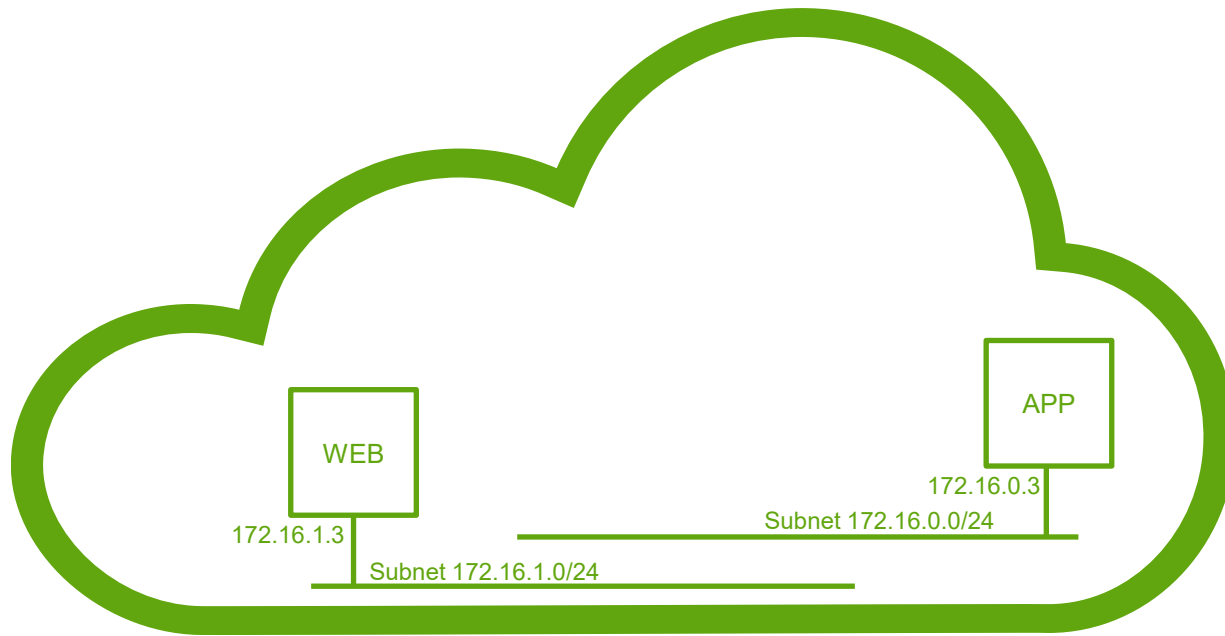
VPCs are instantly created via UI or API



By default, VPCs can't communicate with each other



How does it work?

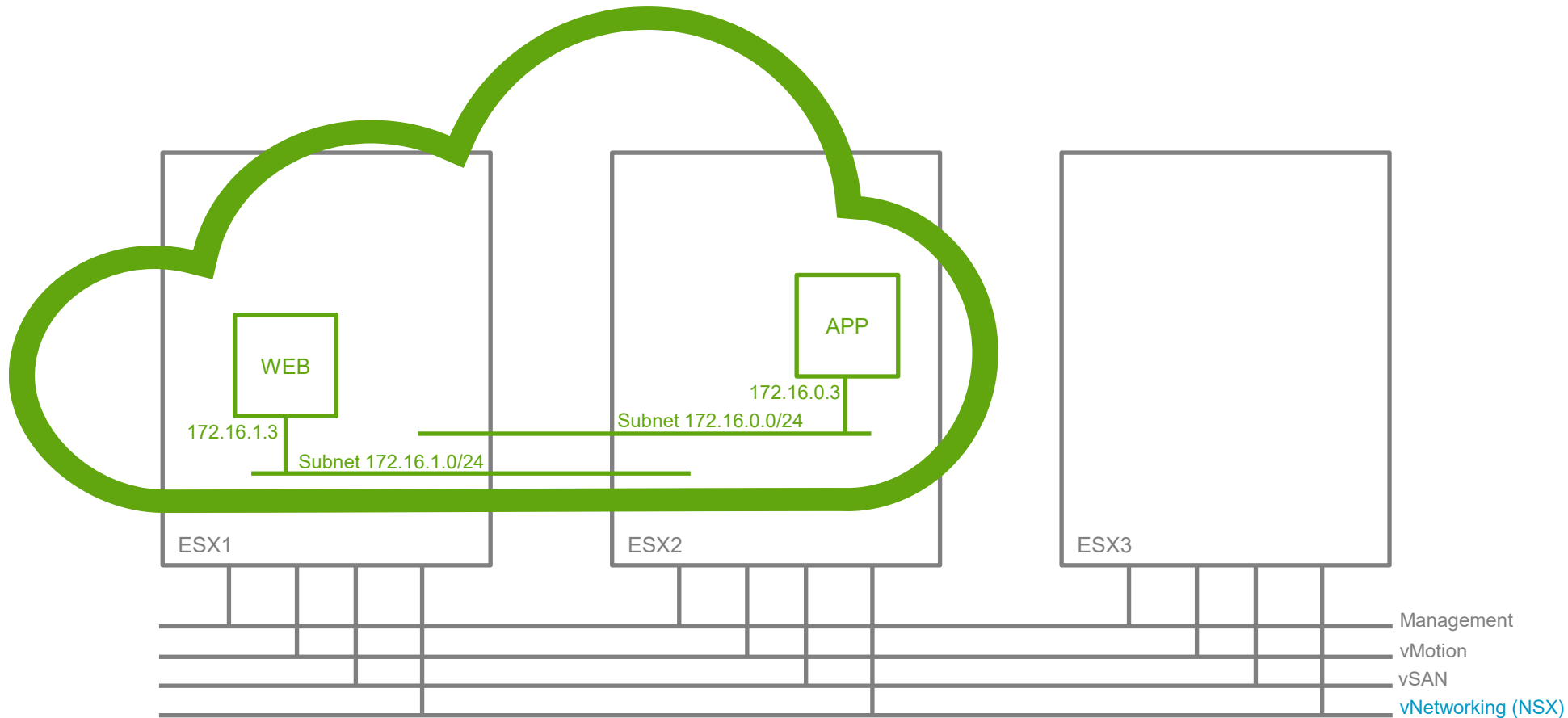


ESXi hosts are configured for compute, storage and networking

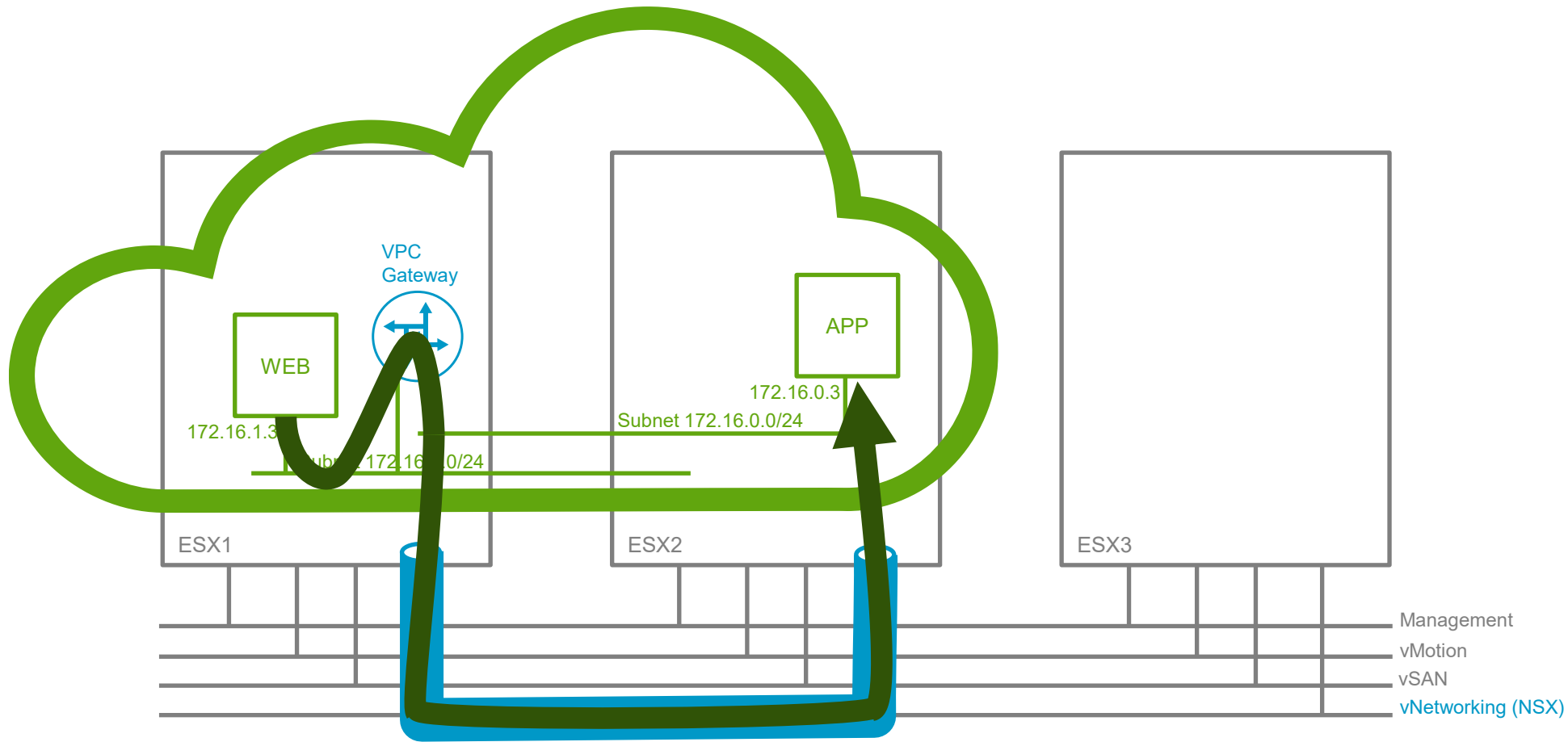

VMware
vSphere®


VMware
vSAN™

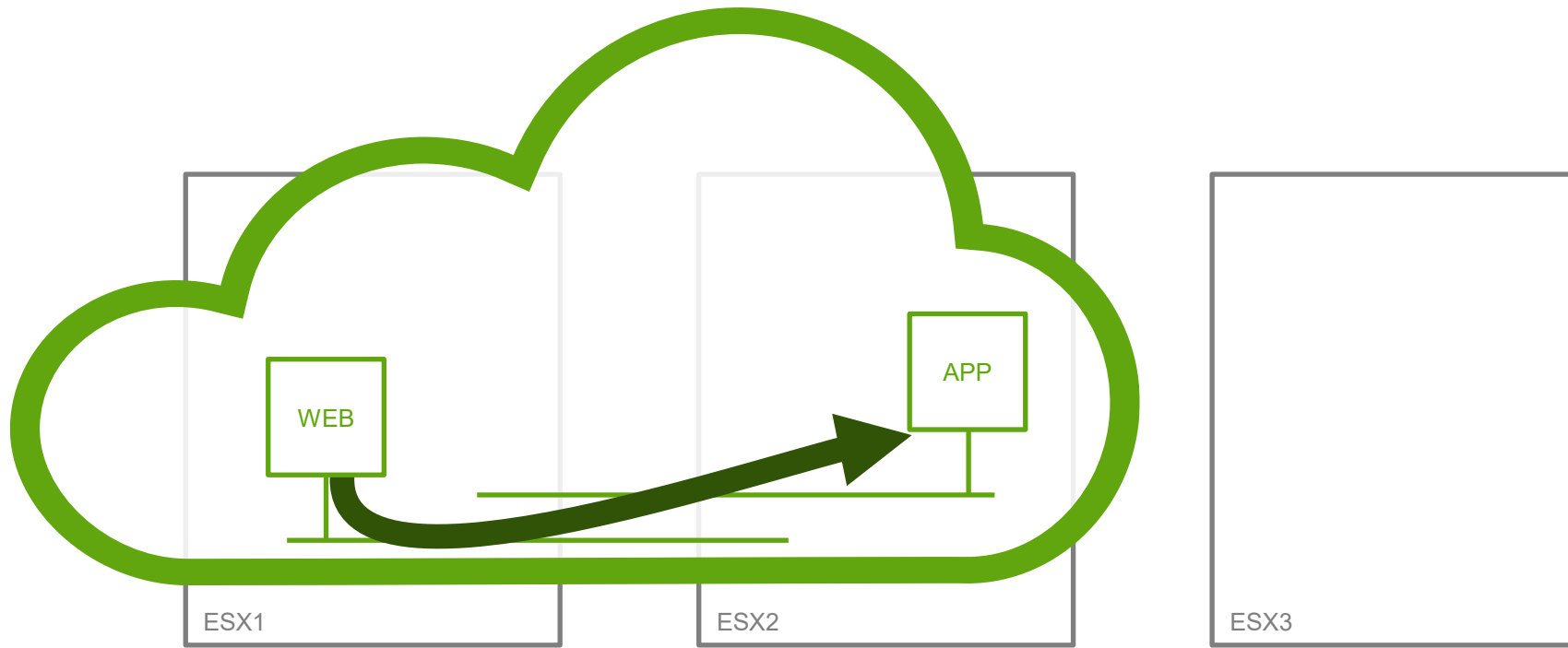

VMware
NSX®



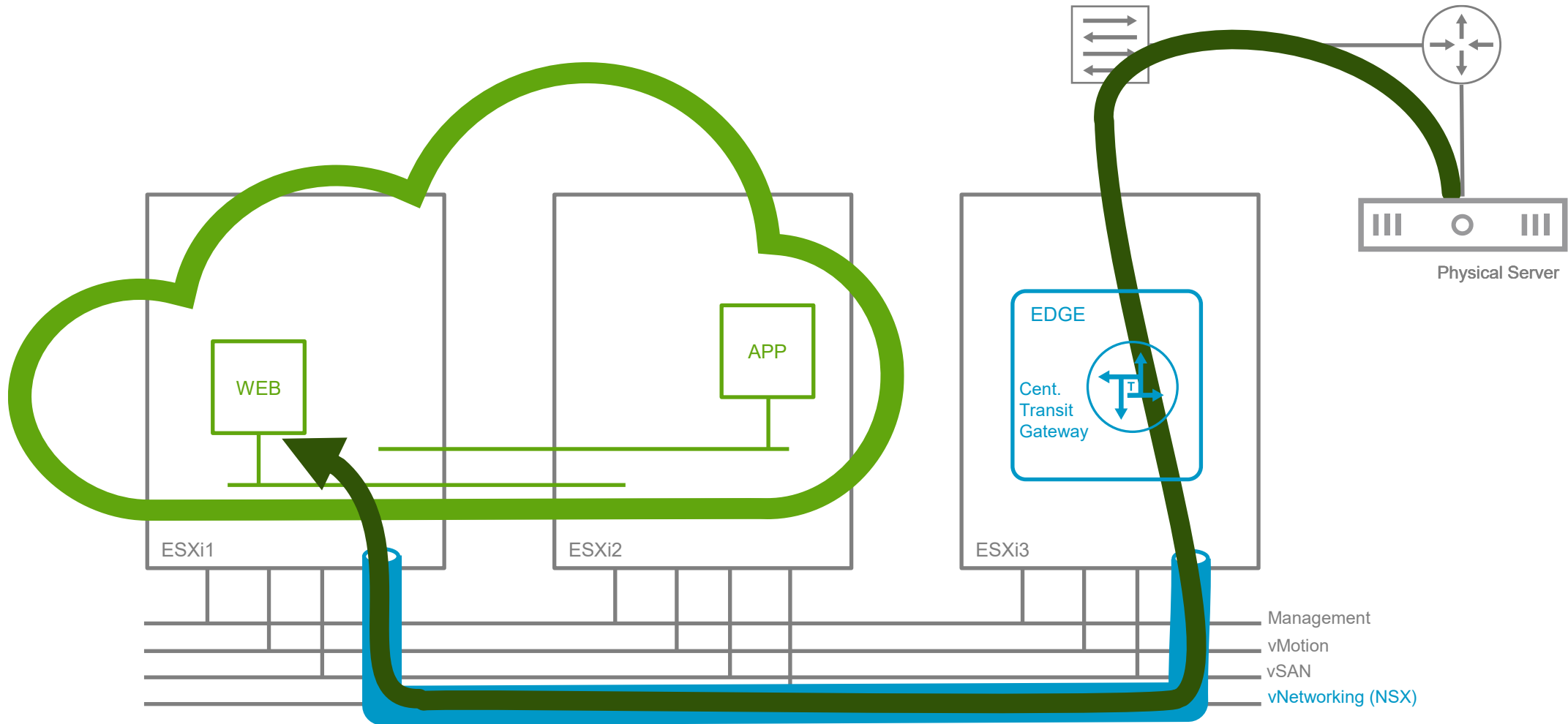
NSX is performing virtual routing and switching



What matters... there is connectivity within the virtual cloud

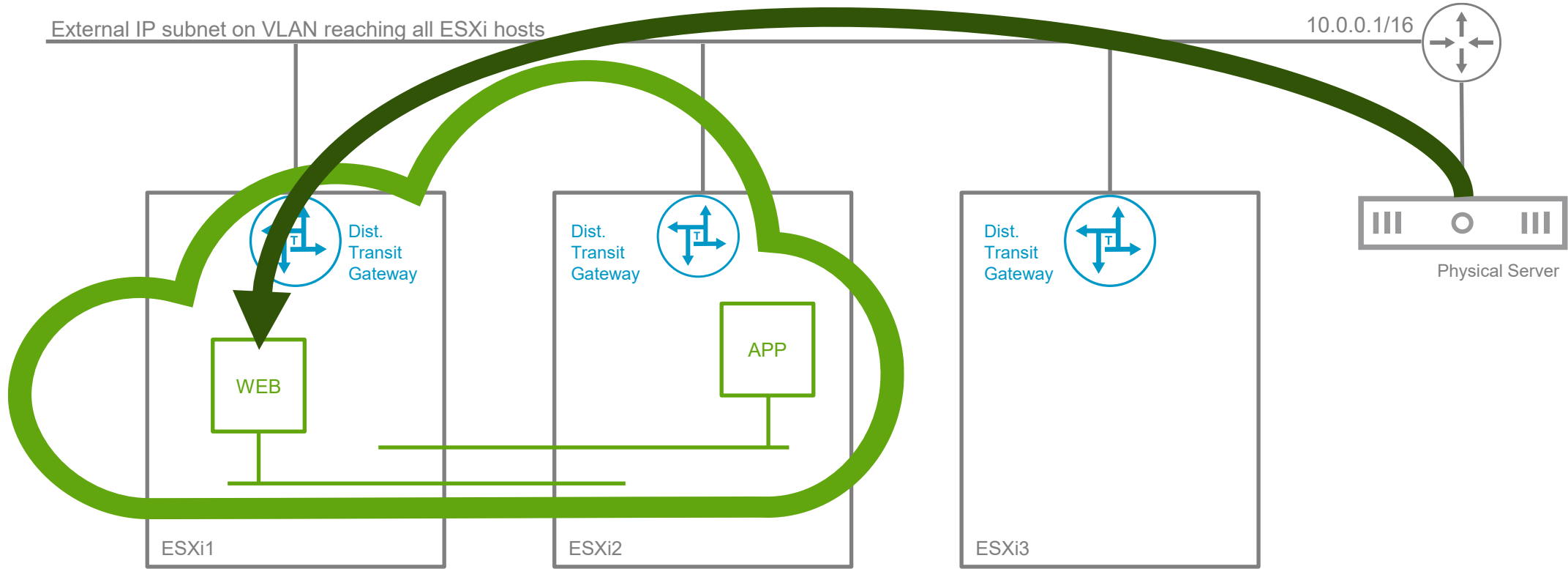


Traditional option 1: Centralized Transit Gateway on edge VM



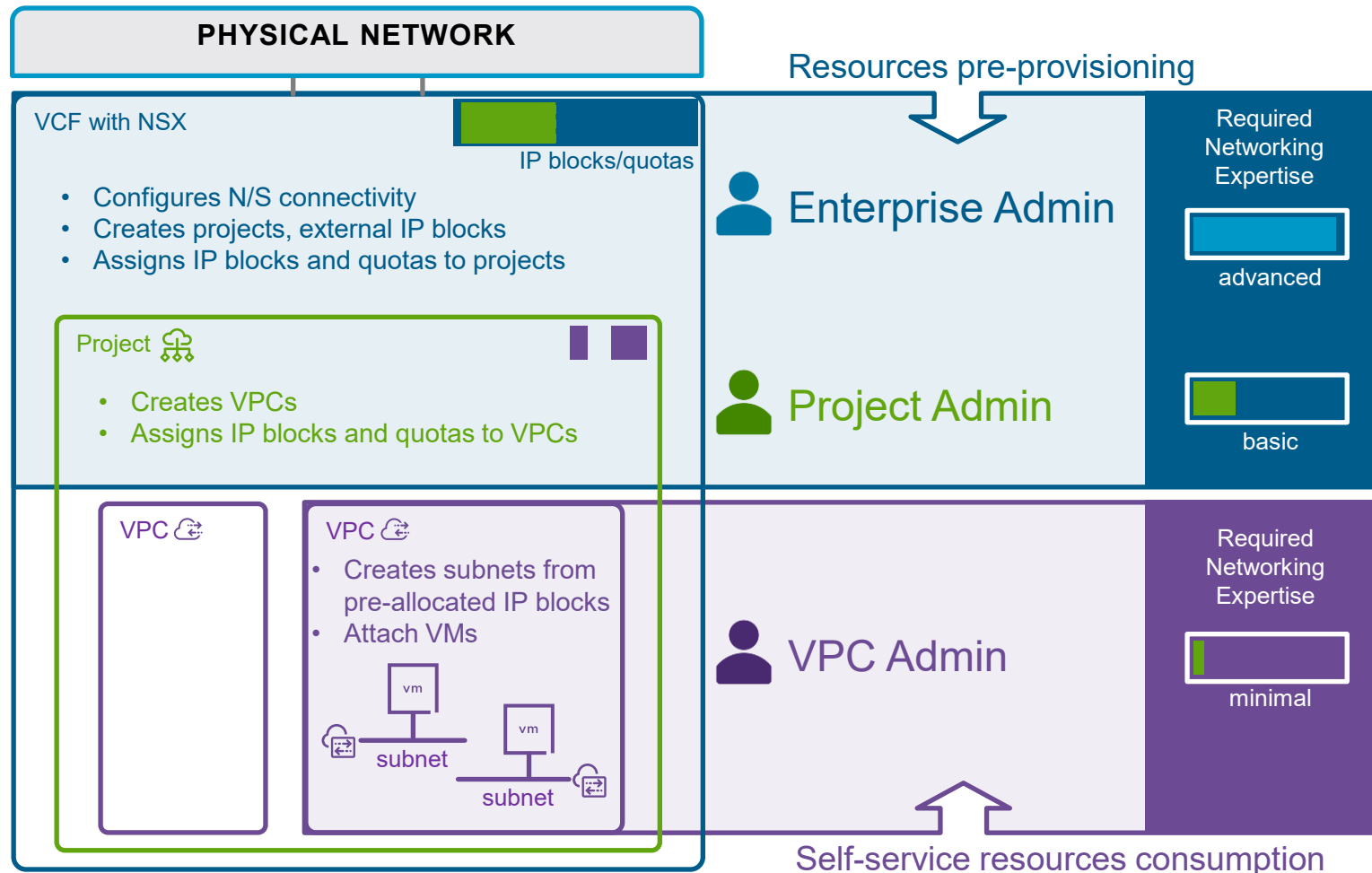
New option 2: Distributed Transit Gateway on each ESXi host

New in
VCF9



Simple Networking with Virtual Private Clouds (VPCs)

Consistent implementation of Virtual Private Clouds (VPCs) across the platform



Clear role definition allows self-service networking

Enterprise Admin:

- Owns the physical infrastructure

Project Admin:

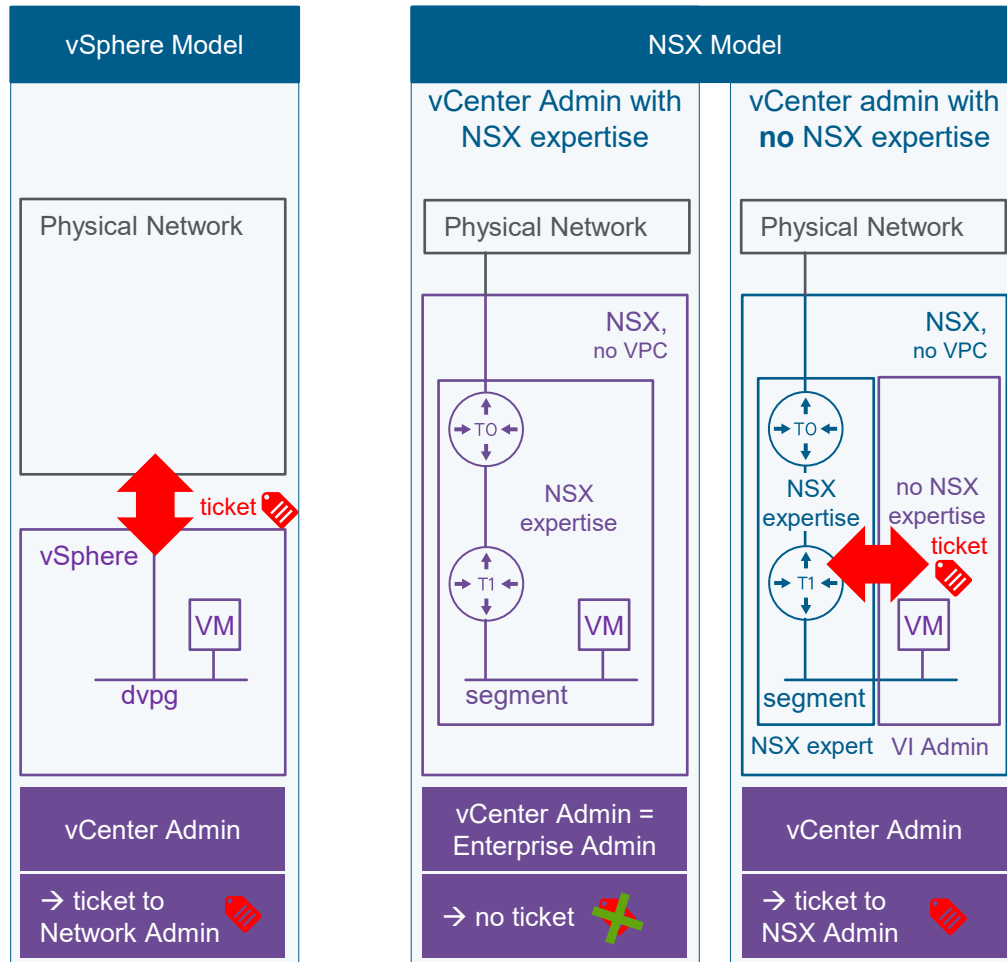
- A tenant
- No direct access to physical network

VPC Admin:

- End user
- Simple, self-service networking

VPC Roles Benefits Go Beyond Multi-Tenancy

Example: deploying a network for a new VM

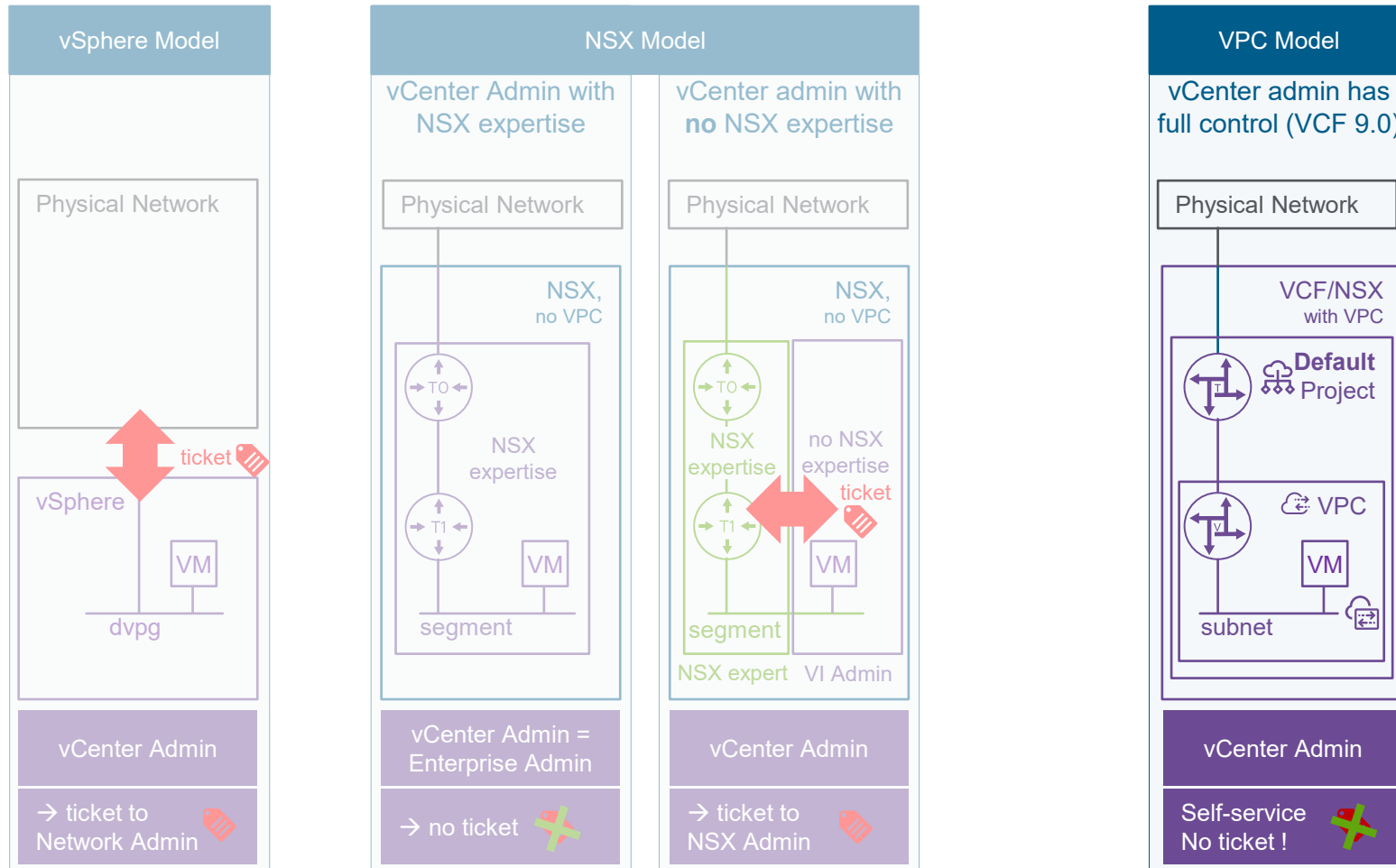


Creating a new network involves the Physical Network Admin

NSX virtual networking operates independently of the underlying physical network infrastructure.

VPC Roles Benefits Go Beyond Multi-Tenancy

Example: deploying a network for a new VM



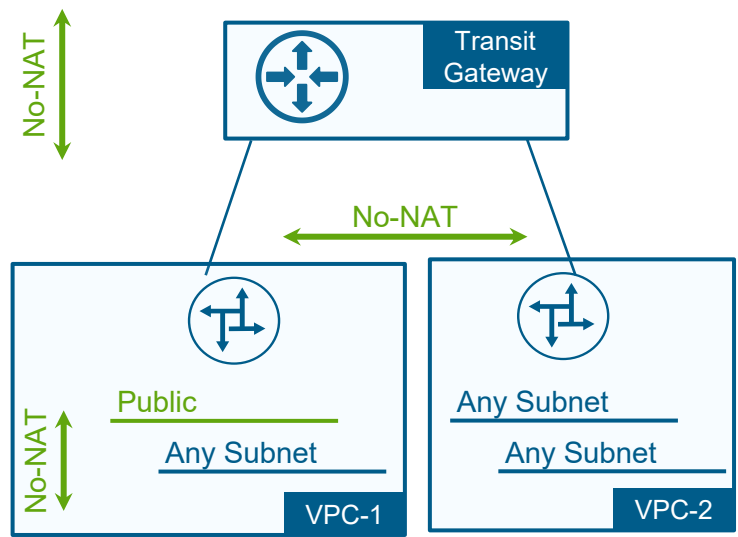
VPC model is adapted to large multi-tenant environments...

And from VCF 9.0 VPC provides simple networking consumption for the users, such as direct consumption from vCenter.

IP Blocks and Subnets

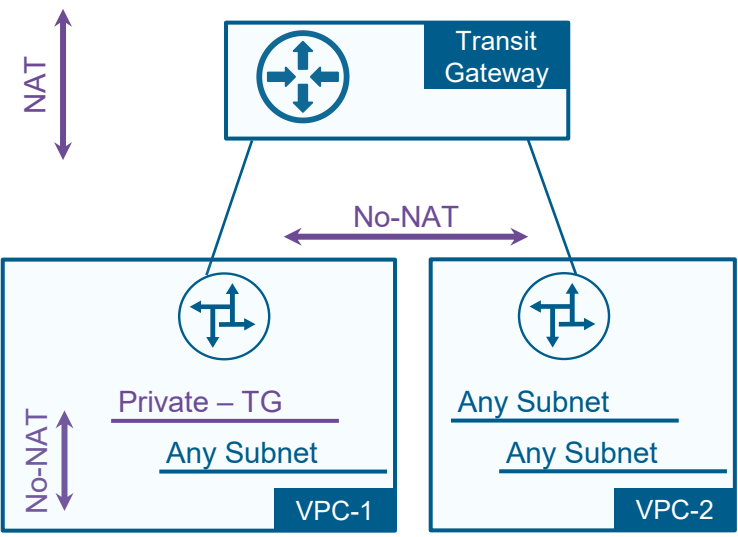
Subnets

Public



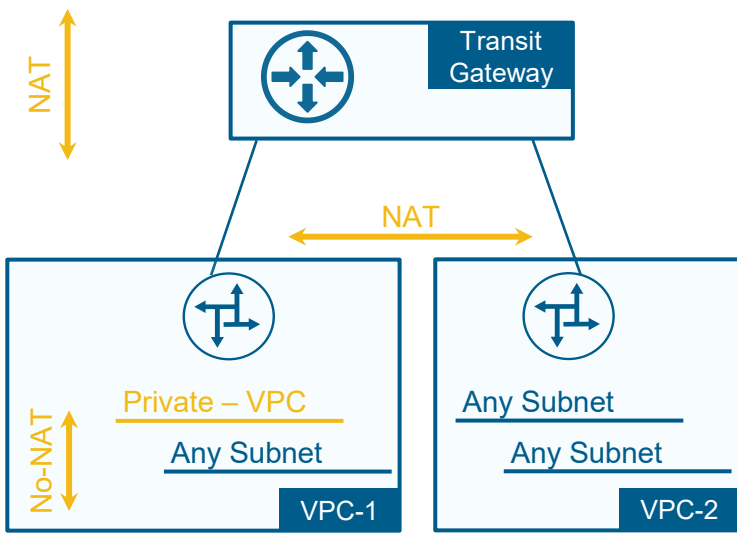
- East-West within VPC: No NAT
- East-West cross VPC: No-NAT
- North of Transit Gateway: NAT

Private – Transit Gateway



- East-West within VPC: No NAT
- East-West cross VPC: No NAT
- North of Transit Gateway: No NAT

Private – VPC



- East-West within VPC: No NAT
- East-West cross VPC: NAT
- North of Transit Gateway: NAT

Version v9.1 and v9.1.1

What's New?



What's New with VCF Networking in VCF v9.1

High Performance Unified Cloud Fabric



EVPN-VXLAN interoperability with the physical fabric

Flexible Connectivity for Advanced Routing Topologies

High Performance access to NVIDIA Connect-X and BlueField adapters

Enhanced VPC Connectivity and Services



VPC Policy-based Connectivity using Communities

IP Address Management (IPAM) for Cloud Consumption

Enhanced VPC Network Services

Native Networking for VKS workloads



Traffic Isolation with Secondary Network Interfaces

Flow Analytics and Path Topology for VKS workloads

Support for Istio Service Mesh

Enhanced Visibility, Planning, and Diagnostics

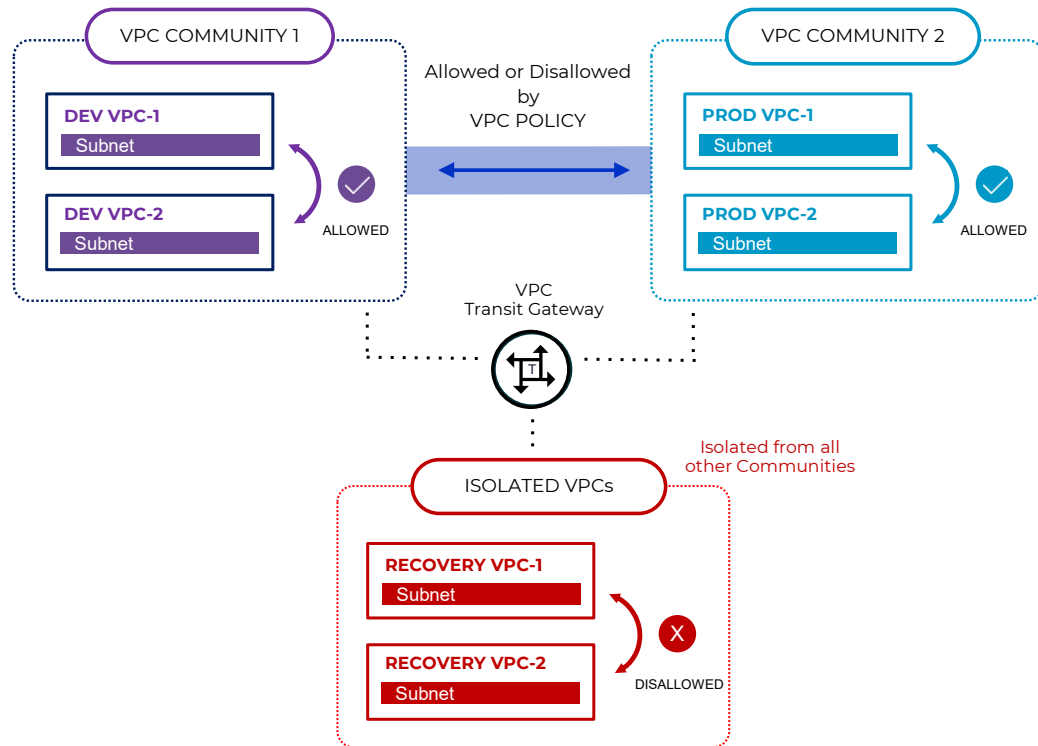


Network Assessment and VPC planning in VCF Ops for networks

Network Diagnostics and Findings in VCF Ops for networks

VPC Policy-based Connectivity for ACC Customers (v9.1)

Enhanced VPC Connectivity and Services



Customer Benefits

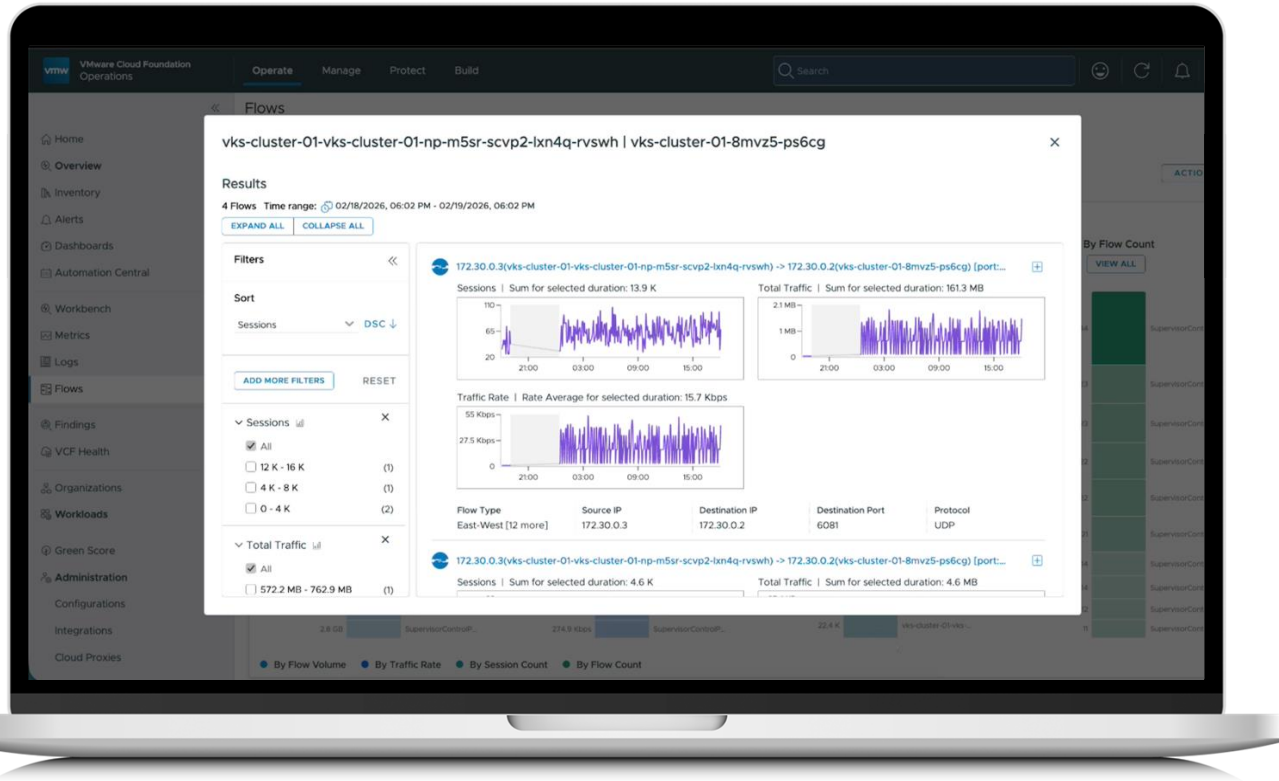
- Customers with the VMware Advanced Cyber Compliance (ACC) add-on can enforce granular VPC-to-VPC and VPC-to-external connectivity using “Community” based grouping
- Simple policy-based isolation without complex firewall rules or external firewalling
- Easier to demonstrate compliance in large regulated environments

Key Attributes

- Built-in isolation between workloads using VPC Communities
- Policy-based connectivity across Communities using VPC Transit Gateway
- Efficient use of infrastructure with fewer VPC transit gateways
- Granular VM level isolation for workloads within a VPC for Cyber Recovery use cases ^[1]

Flow Analytics and Path Topology for VKS workloads (v9.1)

Native Networking for VKS Workloads



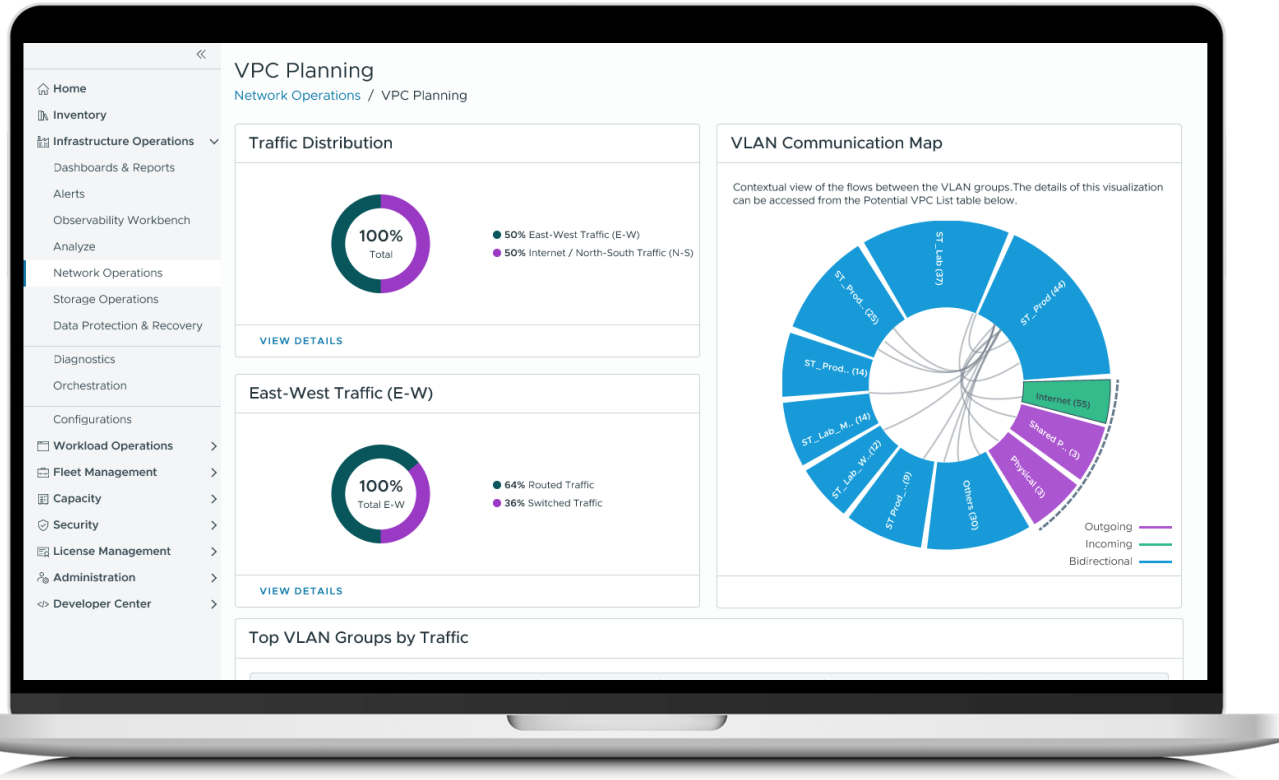
Customer Benefits

- Helps VCF administrators understand traffic patterns and top talkers, and correlate container traffic with VM traffic directly in the VCF Operations console.
- Provides traffic path visibility for troubleshooting performance issues

Key Attributes

- IPFIX support on vSphere Distributed Switch (VDS) and Antrea CNI, enabling granular flow visibility in VCF Operations for networks across VMs and VKS pods for pod-to-pod and pod-to-VM flows.

Visibility, Planning, and Diagnostics



Customer Benefits

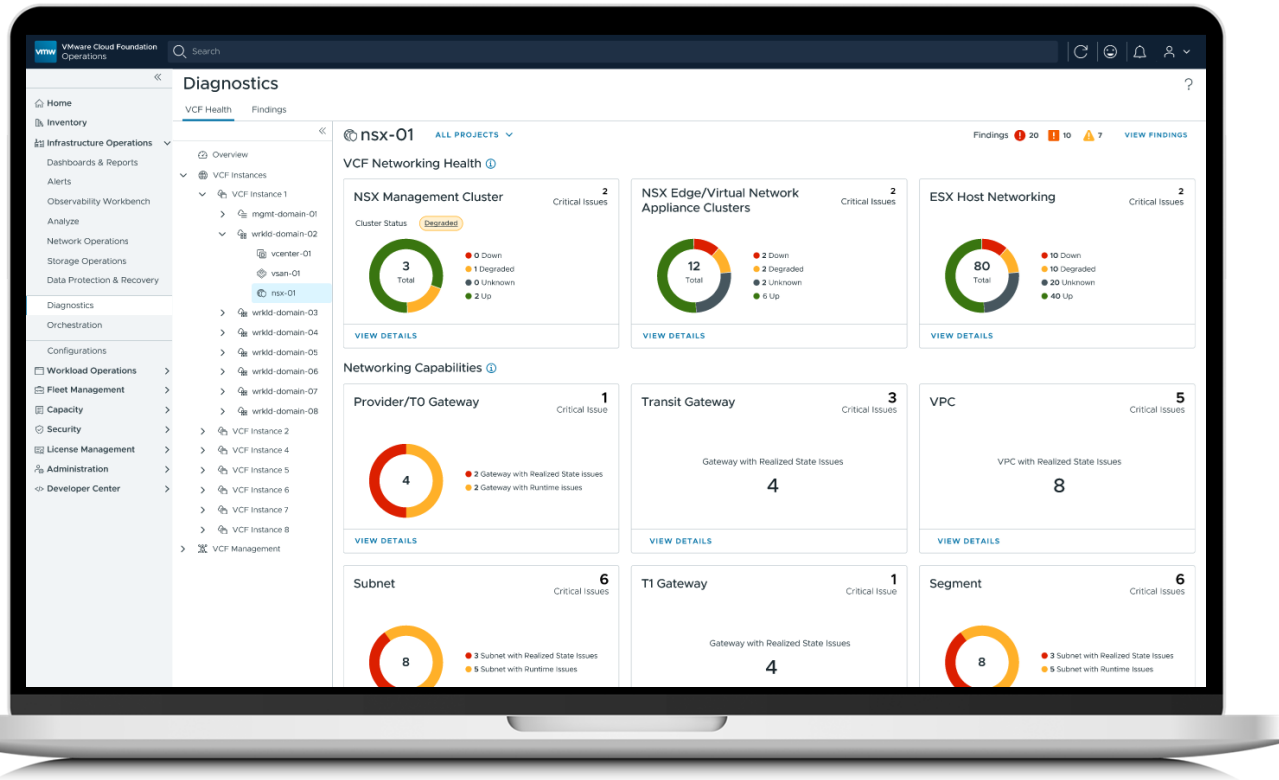
- Easily evaluate and demonstrate the benefits of VCF Networking
- Customers gain visibility into traffic patterns in the private cloud and helps guide them on planning VPCs
- Guided transition from vSphere networking to VPCs and virtual networking

Key Attributes

- **Assessment and Value:** Assess the existing network architecture and configuration including vSphere Distributed Switch (VDS) and vSphere clusters to optimize infrastructure costs
- **VPC Planning:** VPC planning analyzes your existing network infrastructure including VLANs, network traffic patterns, and reachability and provides the users relevant networking parameters required to create VPCs.
- **Migration and Workload Connectivity:** Flow visibility maps applications to VPC subnets and enables workload mobility planning. Users can connect workloads to the VPC Transit Gateway to implement workload connectivity policies recommended during VPC planning.

Network Diagnostics and Findings (v9.1)

Visibility, Planning, and Diagnostics



Customer Benefits

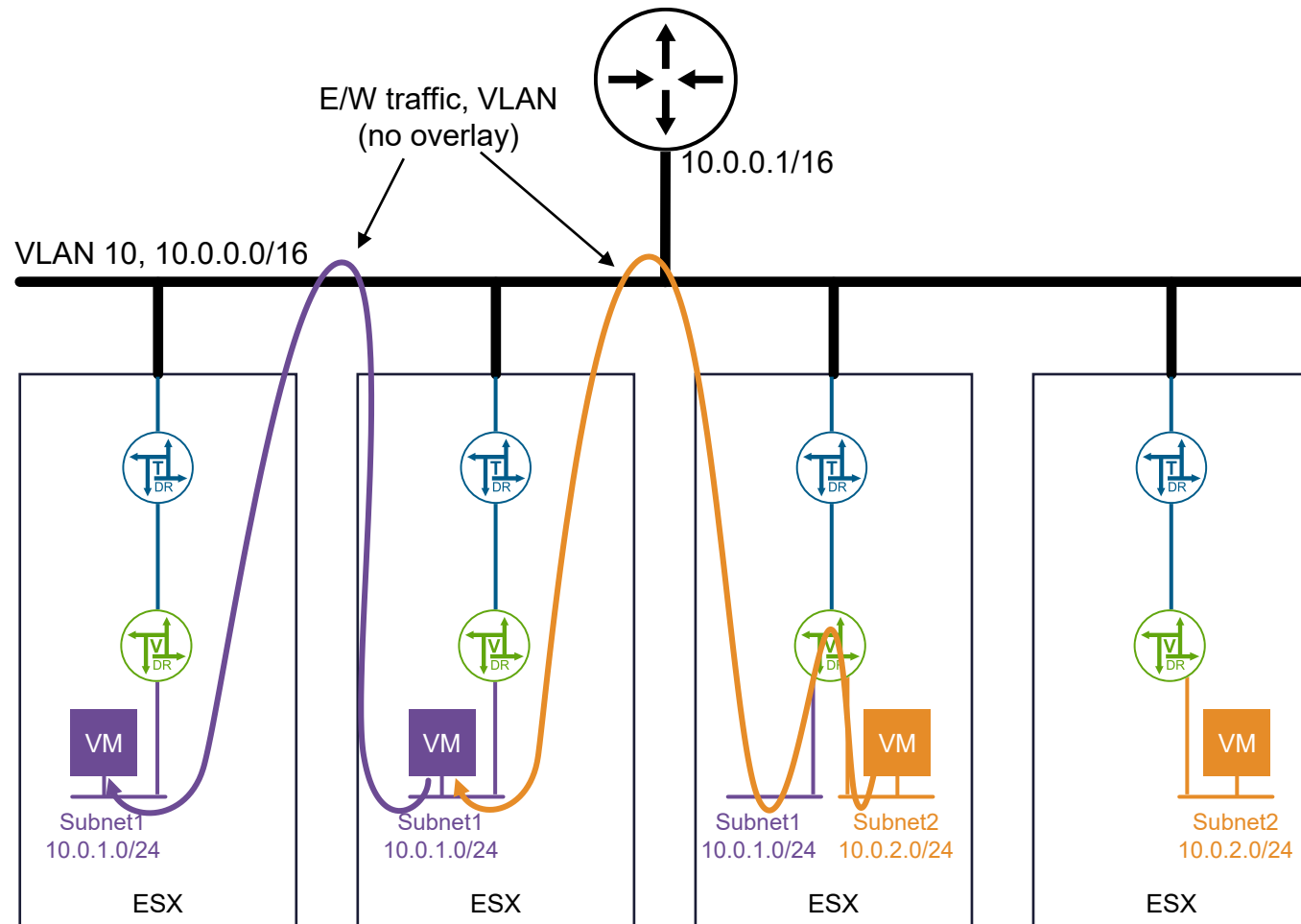
- Improved admin efficiency with fleet-level network and infrastructure visibility and troubleshooting in VCF Operations for networks.
- Triage VCF infra issues quickly with an overall health dashboard that provides infrastructure visibility into critical issues impacting virtual network appliances and capabilities

Key Attributes

- Diagnostics: Out-of-the-box dashboards for network inventory, capacity monitoring, and detailed metrics for the NSX Edge appliance and ESX host networking.
- Users can run integrated ODS runbooks and triage issues quickly.
- A troubleshooting workbench provides VCF wide alerting, metrics, and logging mechanism that centralizes networking alerts, metrics and logs.
- Common Issues captured as part of Findings

VLAN-backed VPCs for VCF Automation and VKS (v9.1.1)

A fallback workload domain deployment option when virtual networking isn't possible



Customer Benefits

Deploy VCF Automation/VKS without configuring a TEP network

No network MTU > 1500 requirement

Supports Virtual Network Appliances for load balancing

Capabilities

Maintain the VPC model and APIs in a VLAN-backed deployment

Limited functionality:

- Public subnets only
- IP unicast traffic only
- No NAT

YOUR FEEDBACK MATTERS

SHARE YOUR THOUGHTS.
SCAN THE QR CODE.



Thank you!



THANK YOU!



Adria Forum 2026

