USDC TECHNOLOGY
Smart Data Center

NSX Cloud

Security & Networking for Hybrid Cloud

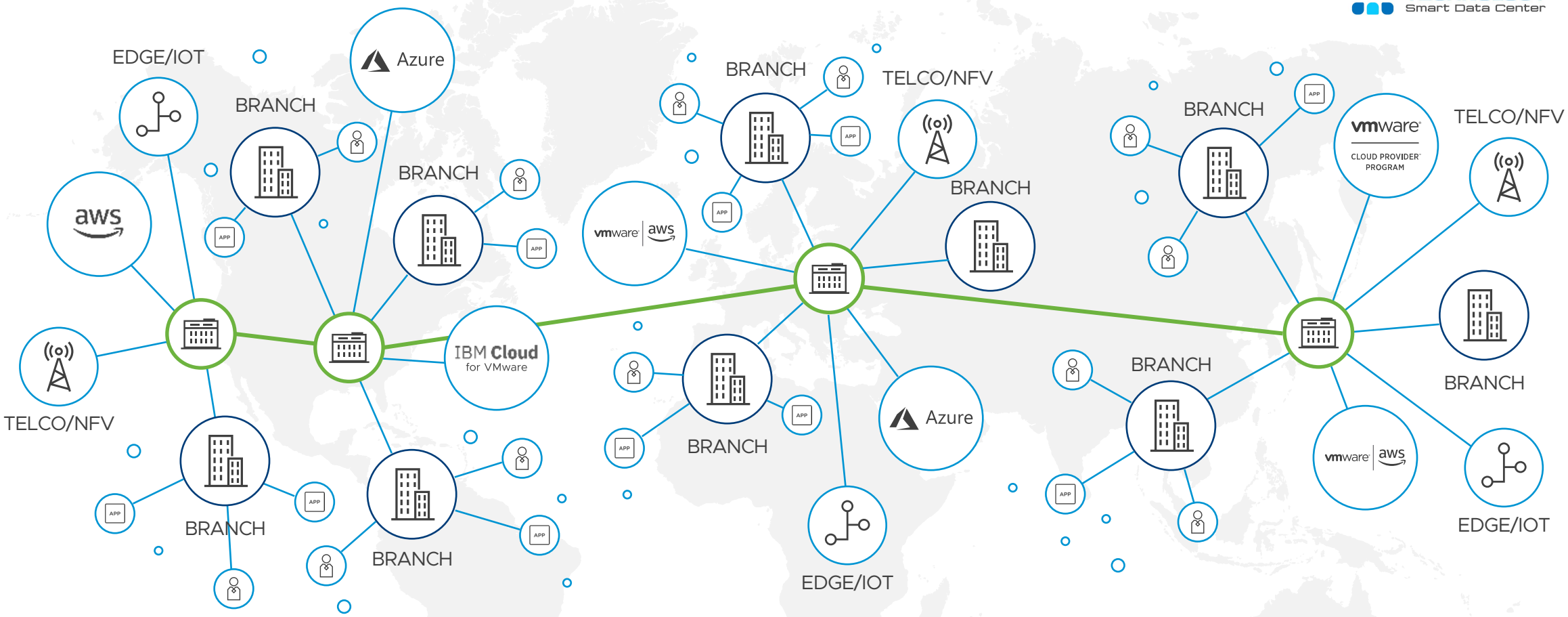
Product Management - NSX Cloud, NSBU, VMware

Sept 2018

vmware®

Agenda

1. Key Challenges in Cloud
2. NSX Cloud - Overview
3. NSX Cloud – Under the Hood
4. Demo
5. Deployment Architectures
6. Summary



The Virtual Cloud Network

Connect and Protect your Business

vmware

VMware NSX Portfolio

The Foundation of the Virtual Cloud Network

NETWORKING AND SECURITY MANAGEMENT AND AUTOMATION

Cloud-Based Management | Workflow Automation | Blueprints / Templates | Insights / Discovery | Visibility

Network Insight
Network discovery and insights

vRealize Automation
End-to-end workload automation

NETWORK AND SECURITY VIRTUALIZATION

Security | Integration | Extensibility | Automation | Elasticity

NSX Data Center
Networking and security for data center workloads

NSX Cloud
Networking and security for Public Cloud workloads

AppDefense
Modern application security

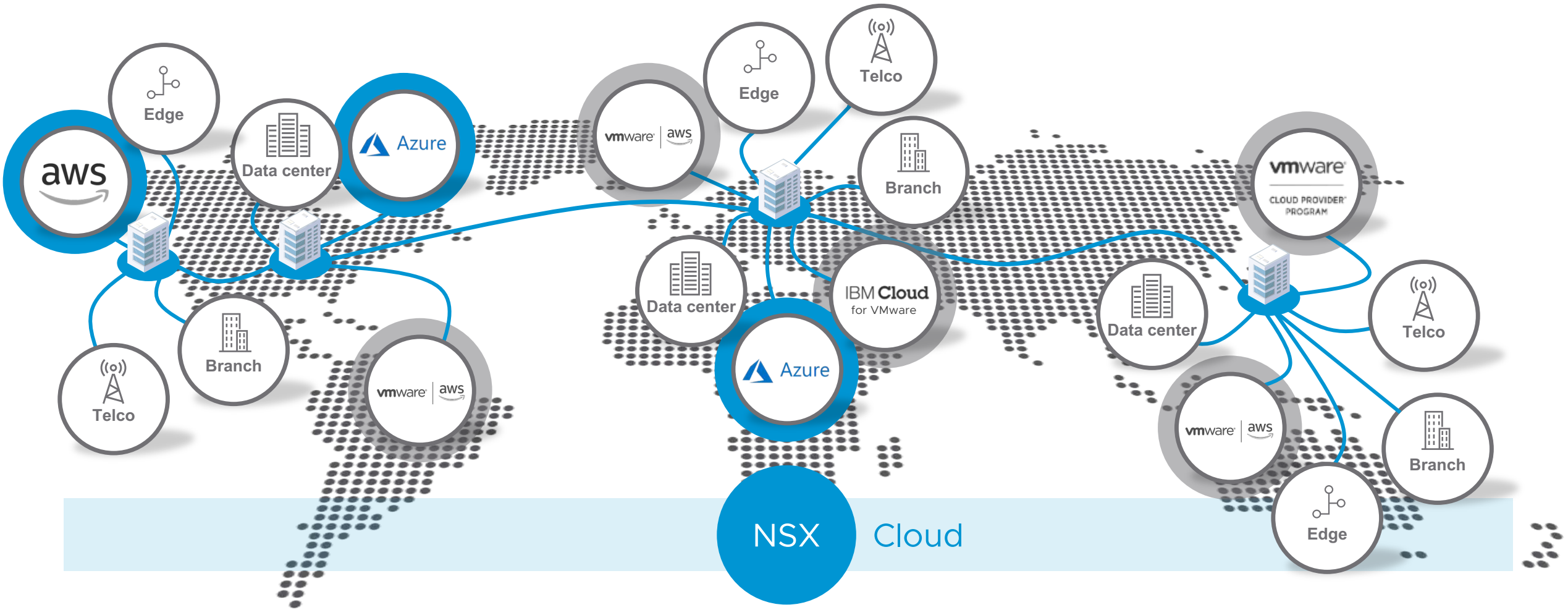
NSX SD-WAN by VeloCloud
WAN connectivity services

NSX Hybrid Connect
Data center and cloud workload migration

vmware

The Virtual Cloud Network

Delivered by VMware NSX



End-to-end consistency from data center to branch to cloud

Native Public Clouds

VMware Clouds

Key Challenges In Public Clouds

Cloud Network Admin

Extending Enterprise network to cloud

Lack of Visibility into Cloud Traffic Flows

Cloud Security Admin

Security policy consistency across hybrid

Leverage enterprise operational tools

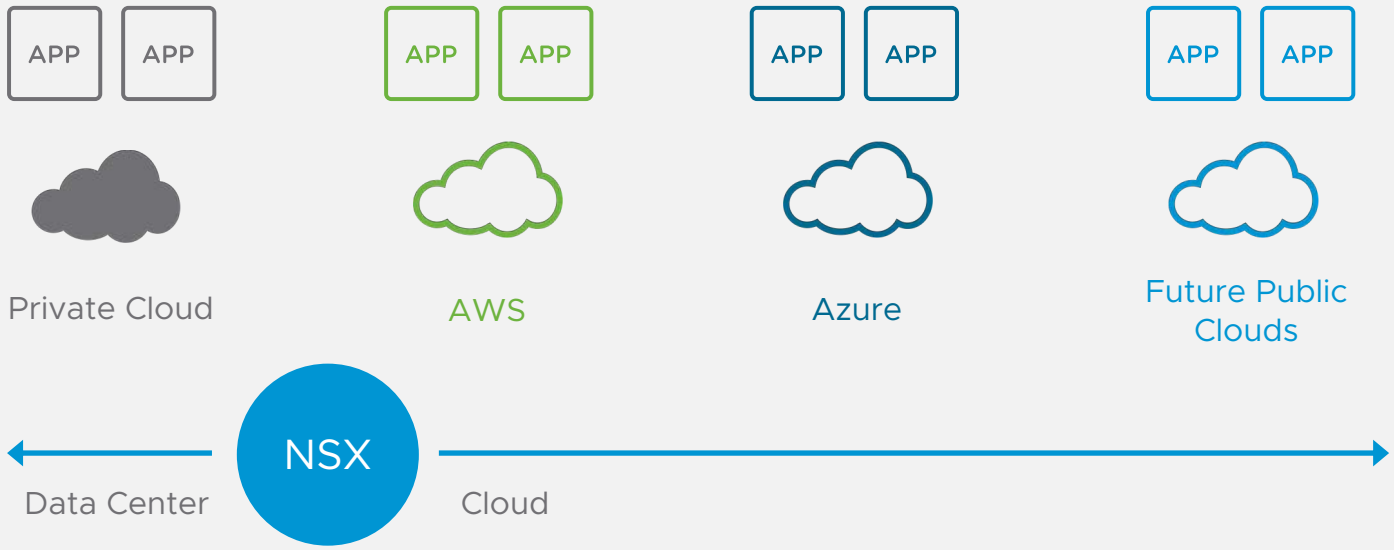
DevOps / Developer

Focus on application Development

Use my choice of Deployment frameworks

NSX Cloud

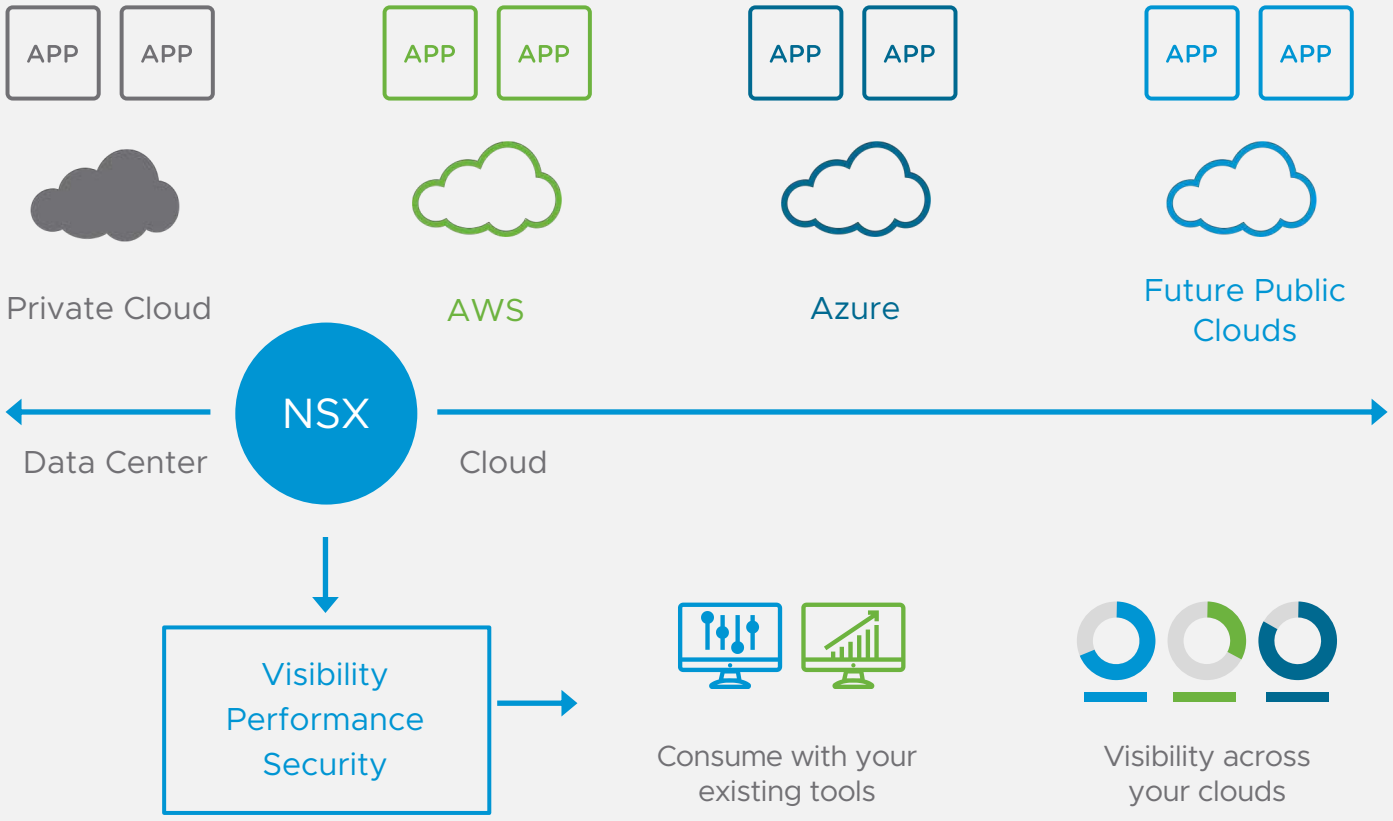
Consistent Networking and Security for Applications



- Visibility across Clouds
- Consistent security policy across clouds
- Precise control over cloud networking
- End-to-end operational control

End-to-end Visibility and Operational Control

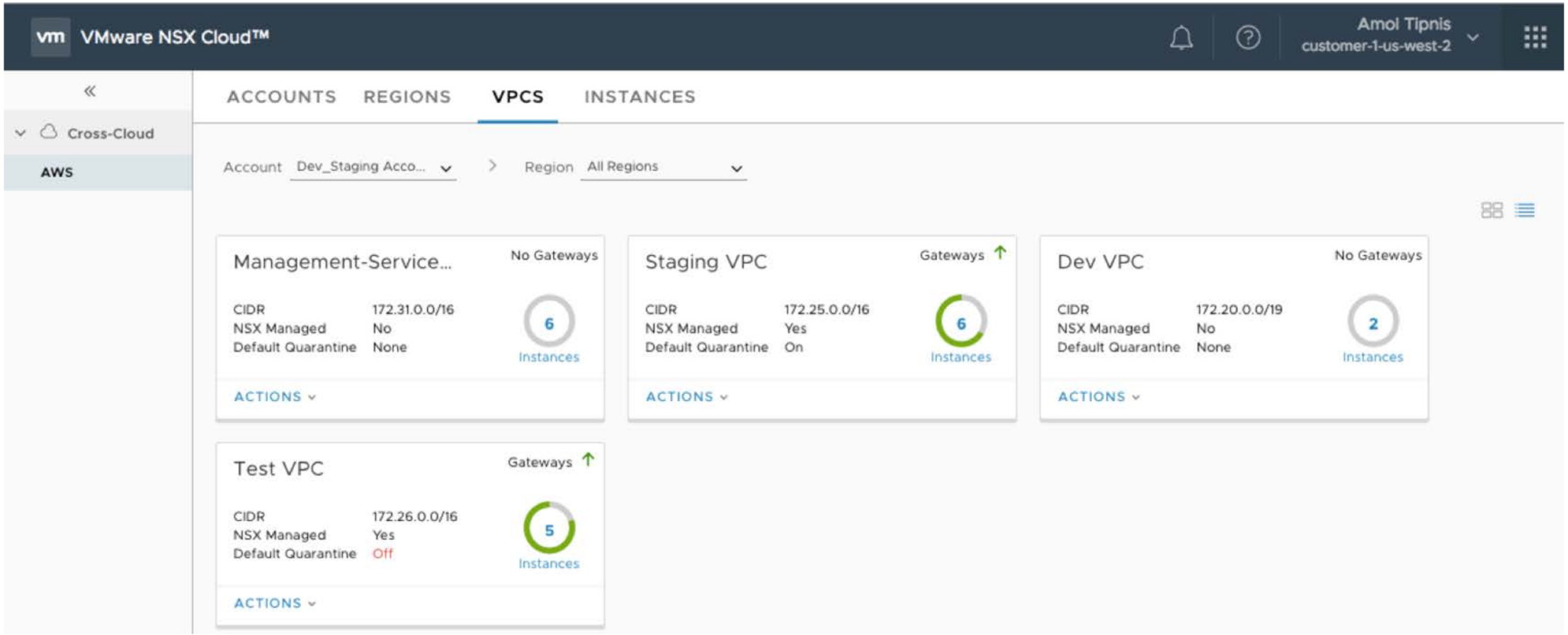
Dramatically Improve Monitoring, Troubleshooting, and Audits



Real-time operational visibility across clouds

Integrate with your existing Day 2 operations tools

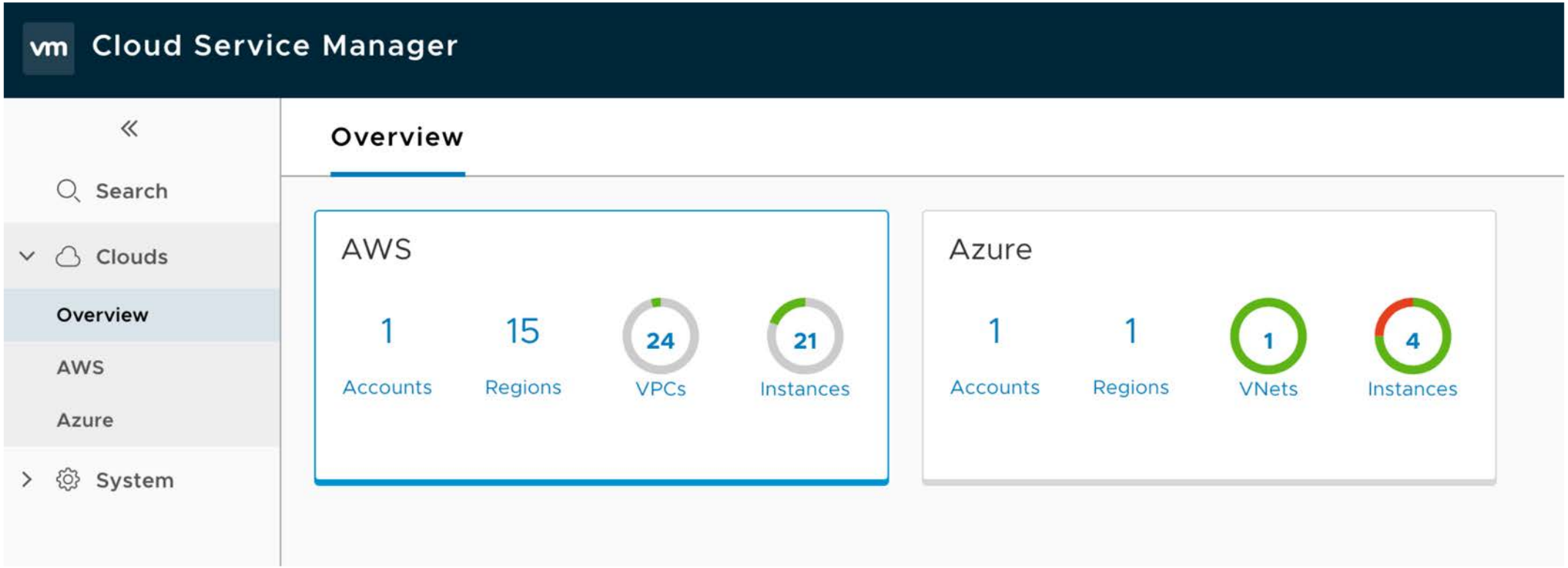
A Single Pane of Glass across all accounts …



Single Inventory View across all accounts and all VPCs

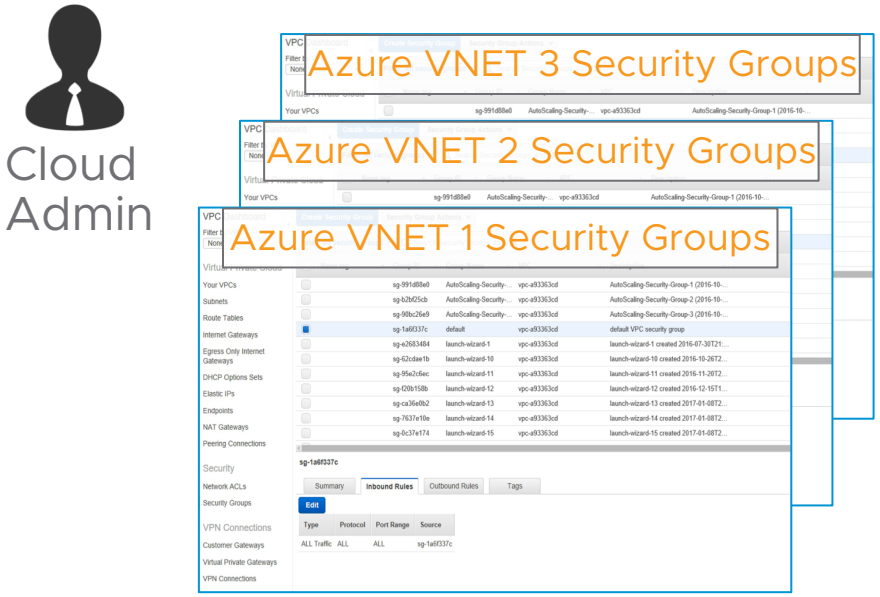
Operational network / security status of every VM enables Rapid Response

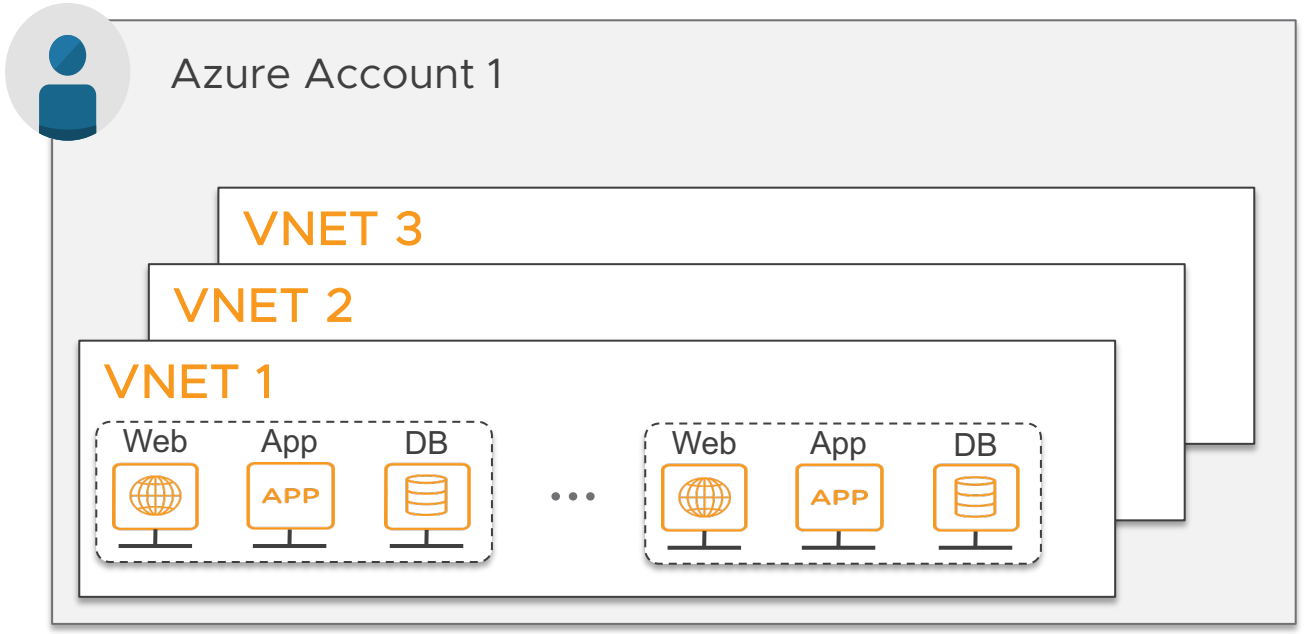
… And across all clouds



Manage and Monitor your cloud across AWS and Azure from a single, consolidated inventory view in NSX Cloud

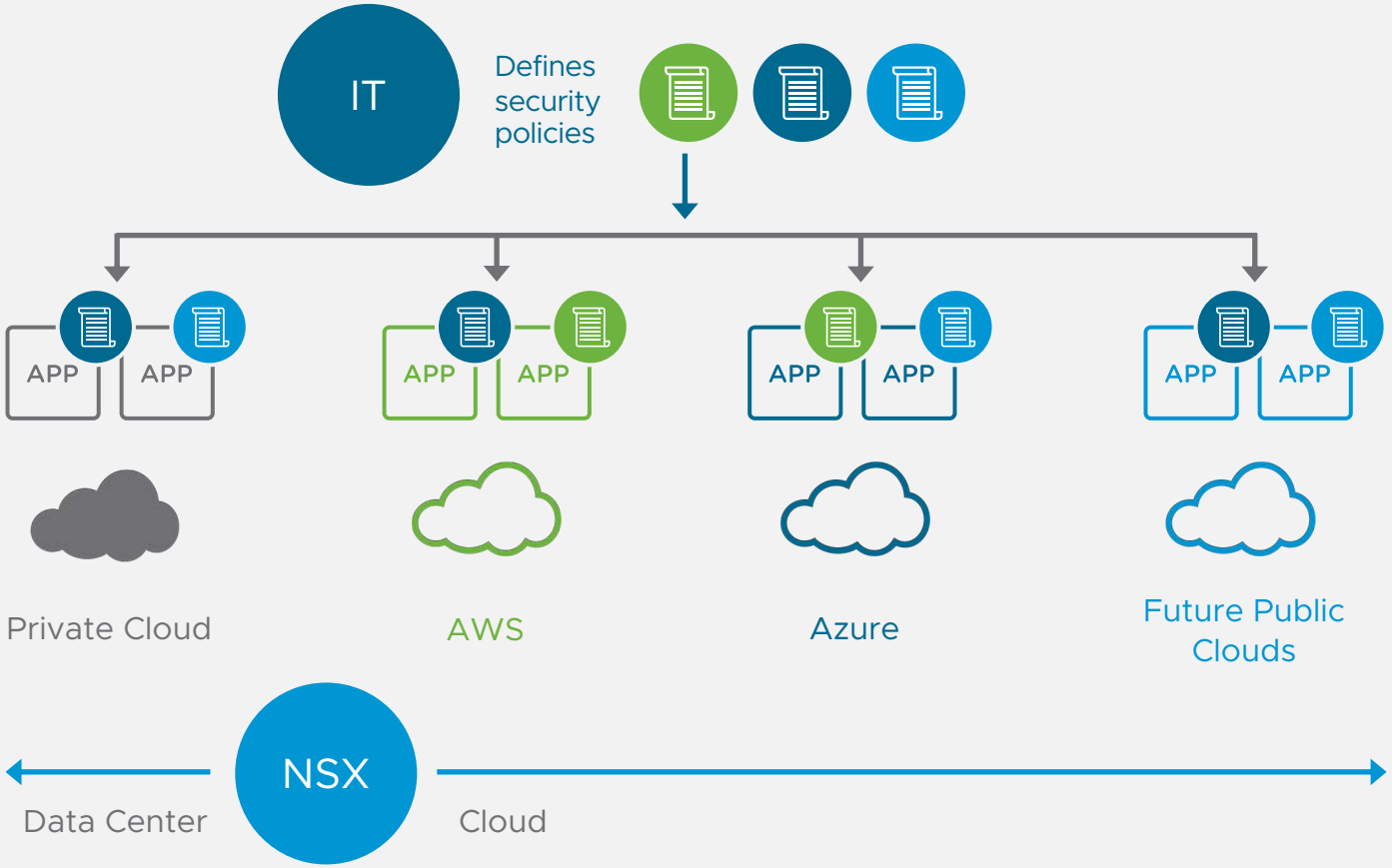
Cloud Security controls are different… with their own limitations





- *Multiple VNETs create multiple security touch-points*
- *Cloud Security Resource Limitations inhibit consolidation*
- *Static Group membership and IP-address rules require coordination at deployment*
- *Cloud Operational framework Inconsistent from on-premise*

Consistent Security Across Clouds



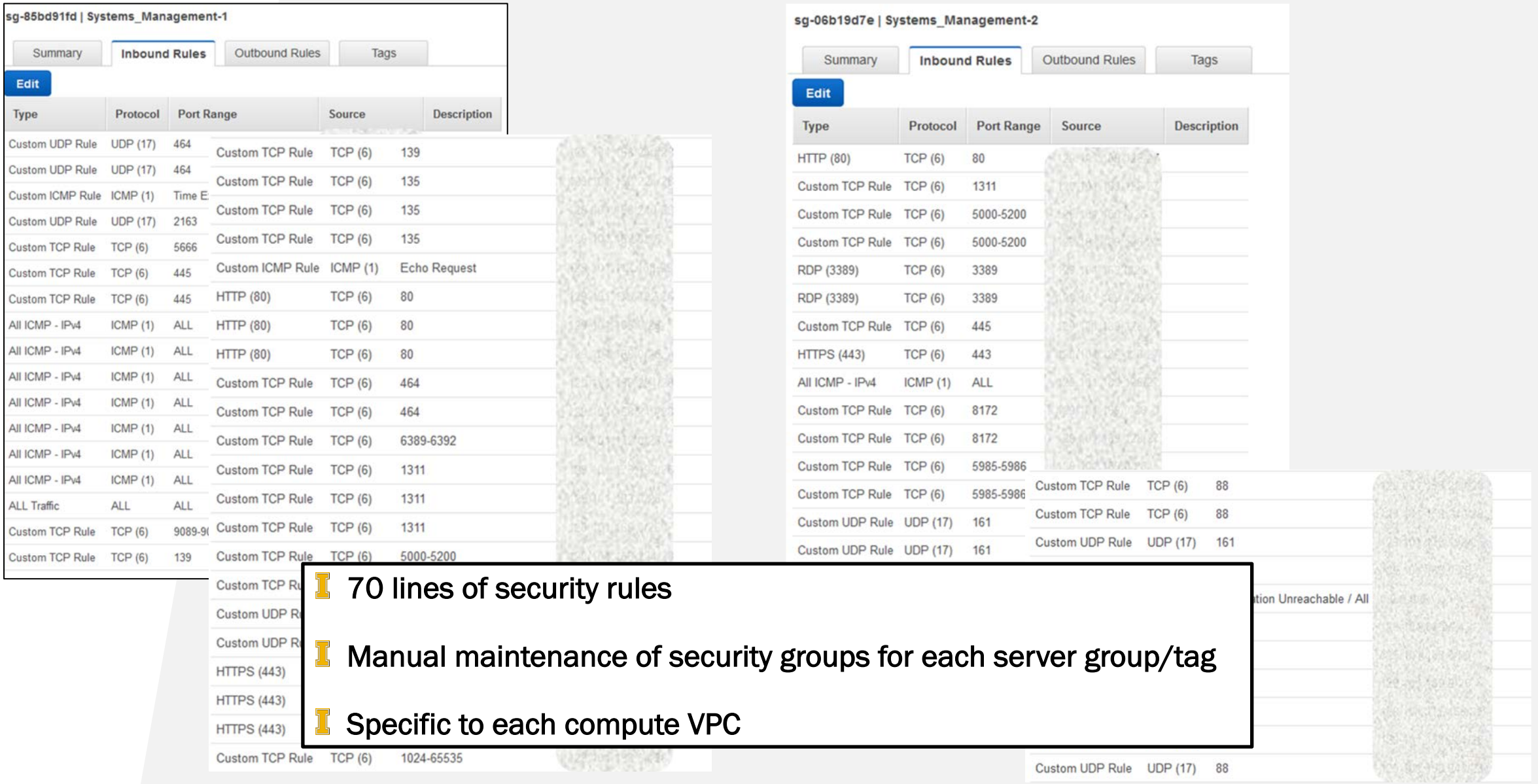
Single Security Policy: define a policy once, then apply anywhere

Rich set of abstractions

Granular enforcement of application workloads

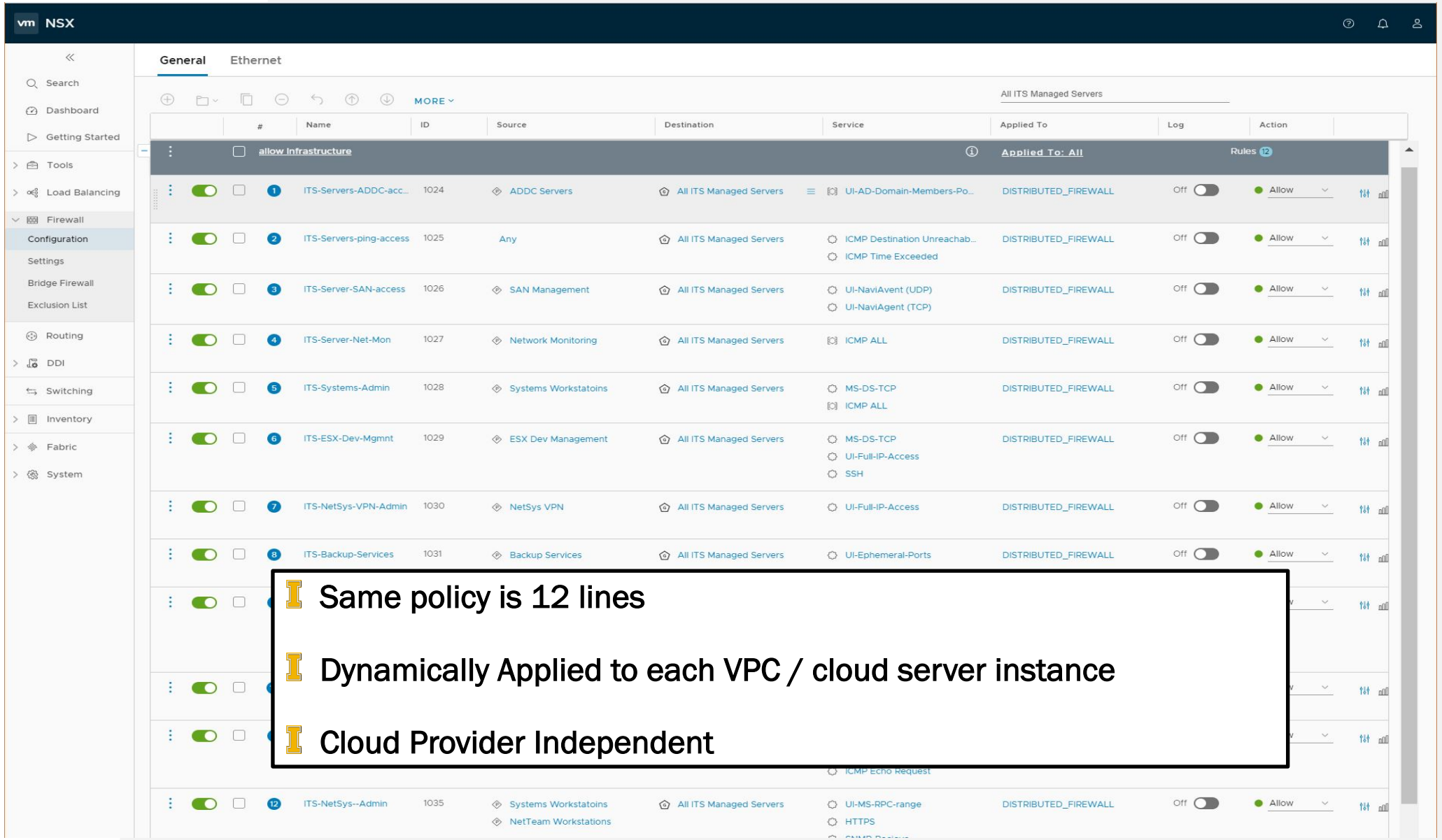
Dynamic security group membership and policies follow workloads as they move

UNIV OF IDAHO FIREWALL POLICY IN AWS



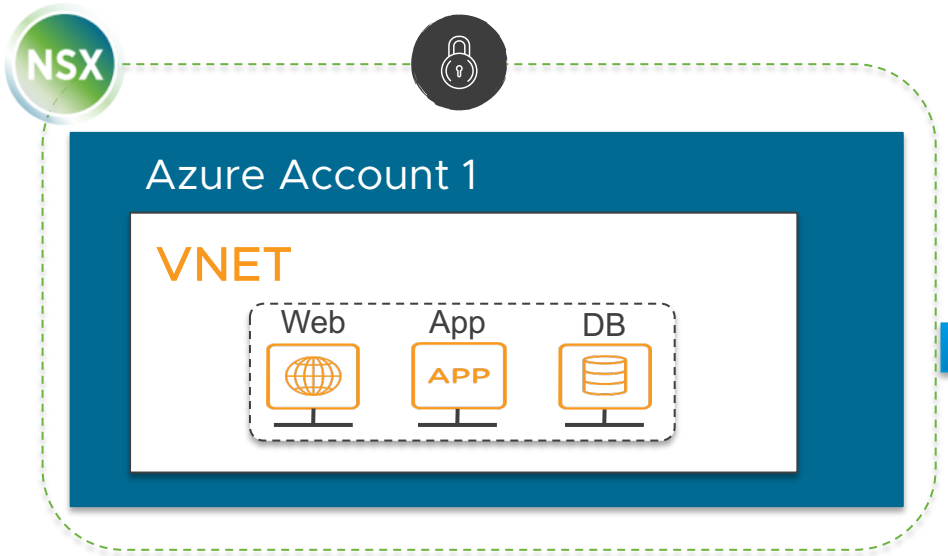
- 70 lines of security rules
- Manual maintenance of security groups for each server group/tag
- Specific to each compute VPC

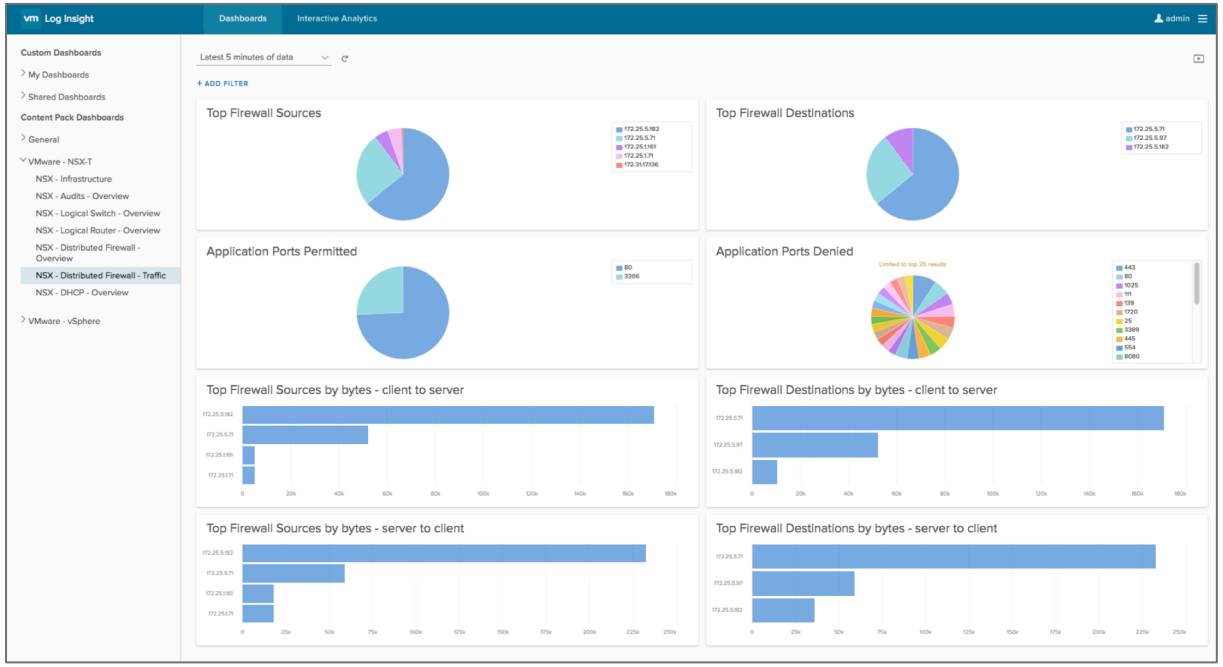
FIREWALL POLICY IN NSX CLOUD



- Same policy is 12 lines
- Dynamically Applied to each VPC / cloud server instance
- Cloud Provider Independent

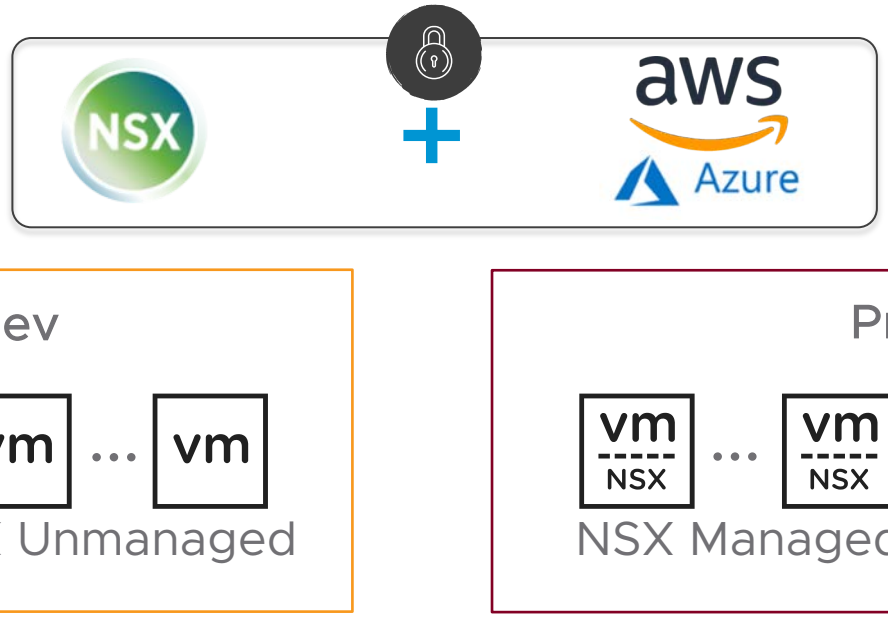
Real Time Operational Visibility Into Firewall Rule Invocations





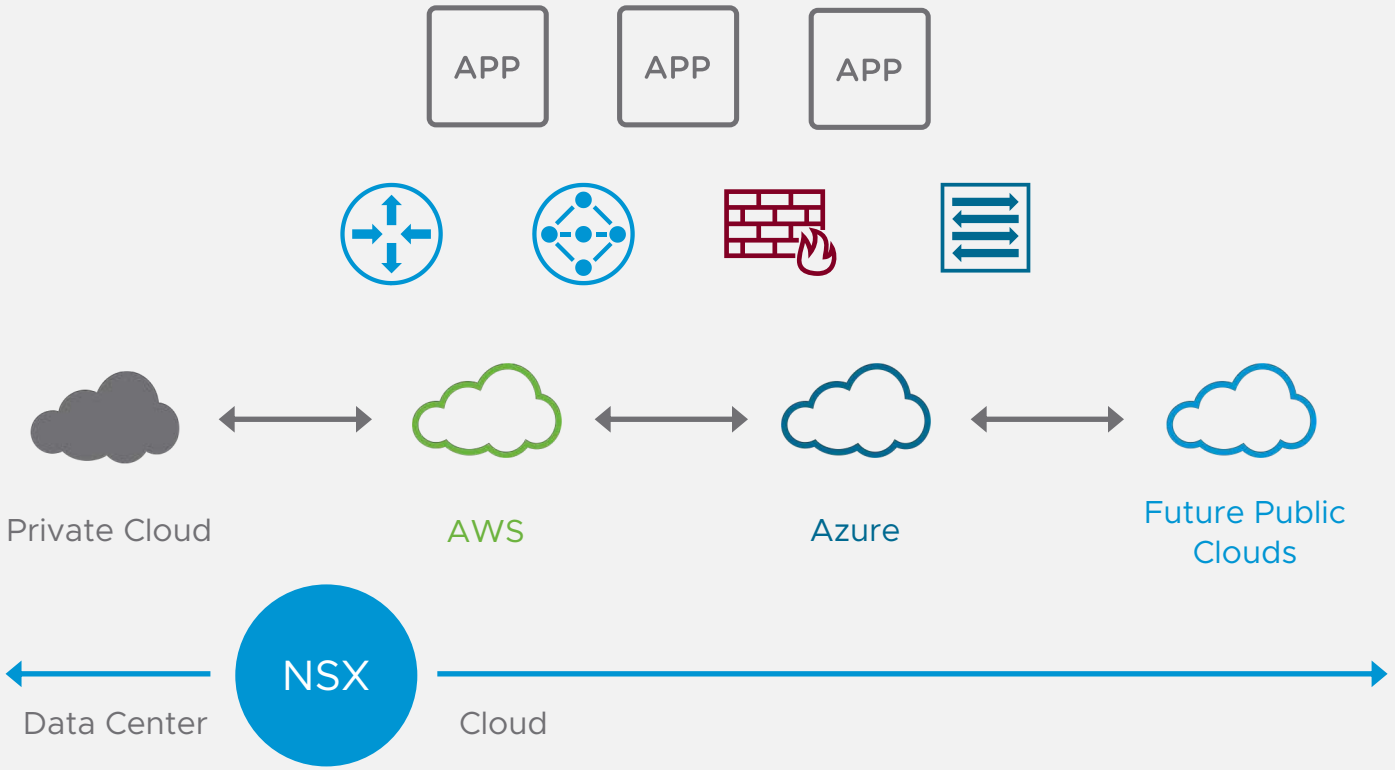
- *Route firewall logs to **industry-standard syslog**, leverage SIEM tool of your choice*
- ***Real-time Operational visibility** into your cloud security posture*
- ***Operationally consistency** with your on-premise security environment*

Defense in Depth through Default Quarantine



- **Multi-layered security** through NSX and Azure security groups managed by NSX
- Fully Configurable to each VNET with exclusion lists
- **Best of Both Worlds** – Greater agility for test & dev, higher structural integrity for production

Precise Control over Cloud Networking



NSX works alongside native public cloud services

Built-in VPN provides immediate TCO reduction

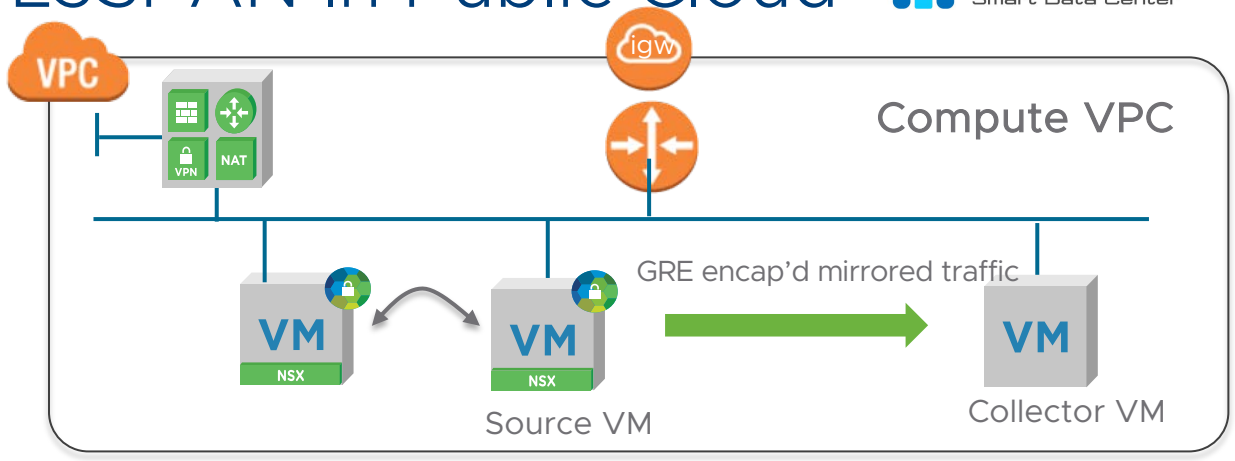
Consistent, automated provisioning of apps or services

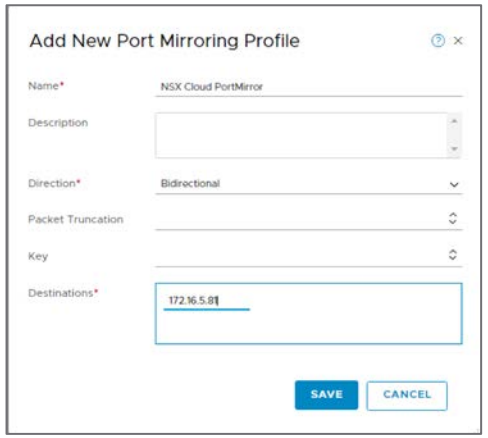
Real Time Operational Visibility - L3SPAN In Public Cloud

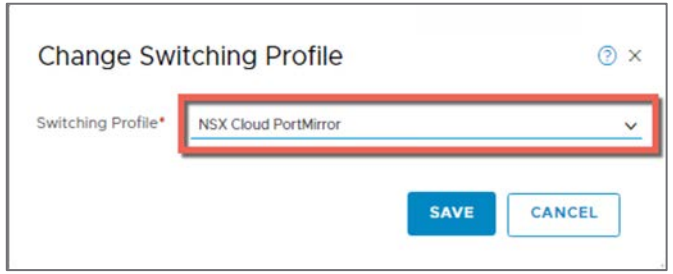
USDC TECHNOLOGY Smart Data Center

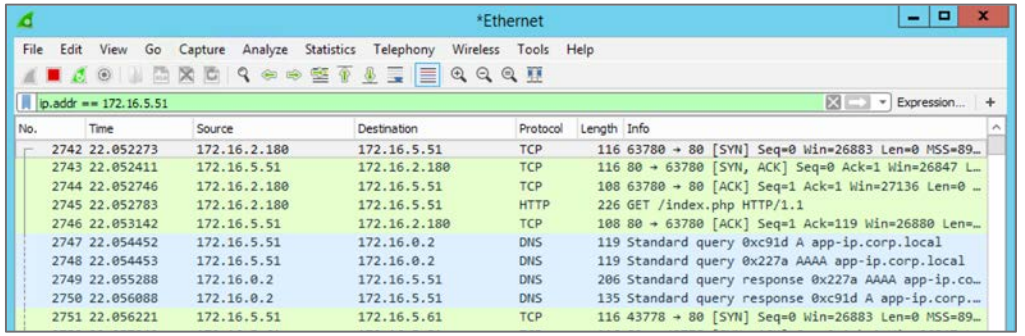
Consistent Operational Visibility – Packets

- Enable NSX L3 SPAN/Mirror on a per Logical port or Logical switch basis using Port-mirroring Switching Profile
- NSX Agent running inside the VM captures the traffic.
- Mirrored traffic forwarded to IP destination (collector) within VPC using GRE
- Supports both, non-overlay and overlay mode of operations
- Initially supported in AWS.





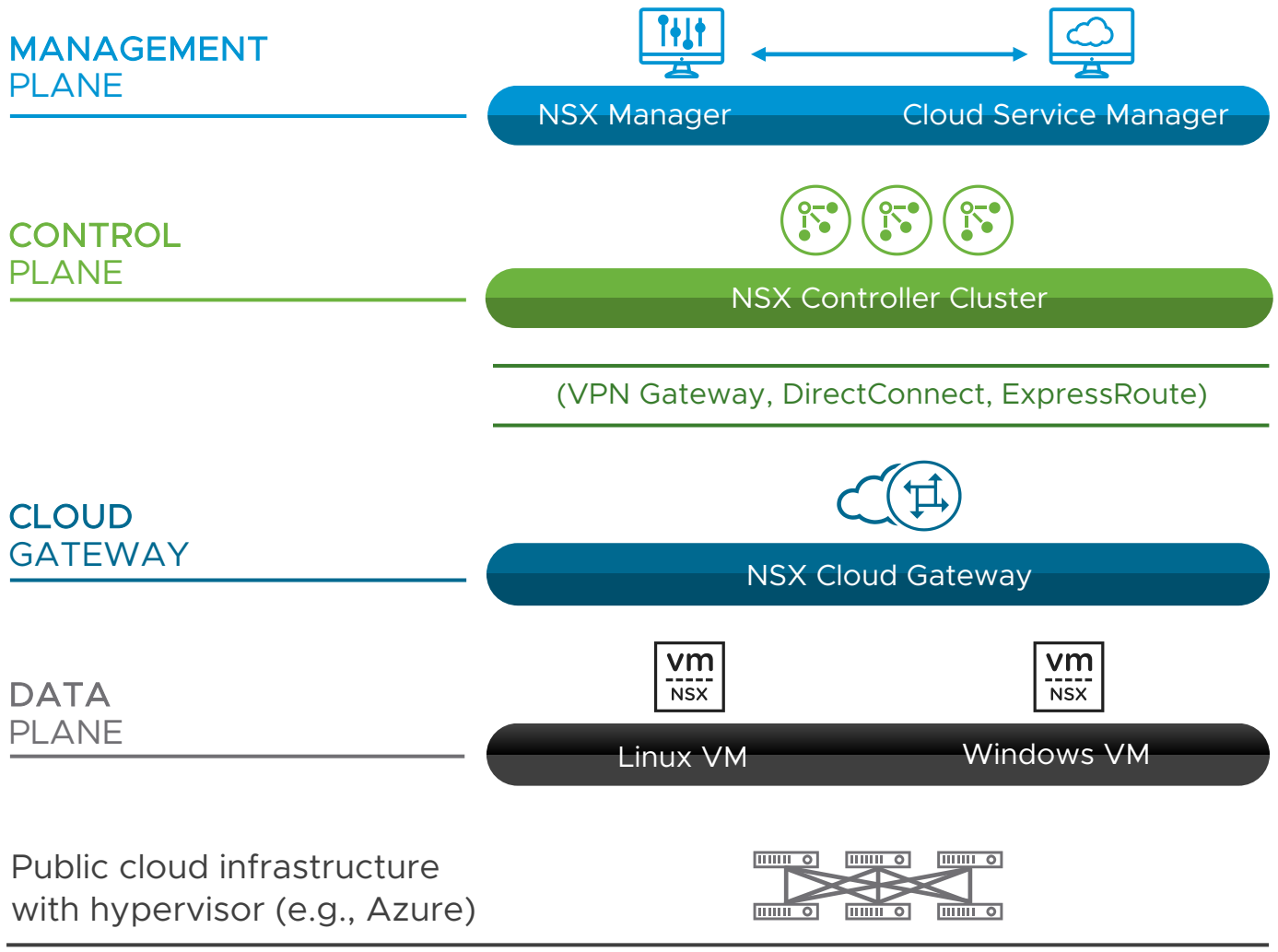




vmware

NSX Cloud – Under the Hood

VMware NSX Cloud – Product Deployment Under the Covers



NSX-T Management Plane and Control Plane deployed in on-premise Data Center

Add Cloud Service Manager to get visibility into your hybrid cloud

Deploy Public Cloud Gateways (PCGs) in cloud VPCs / VNETs

NSX agents auto-deployed with PCG or embedded in application templates

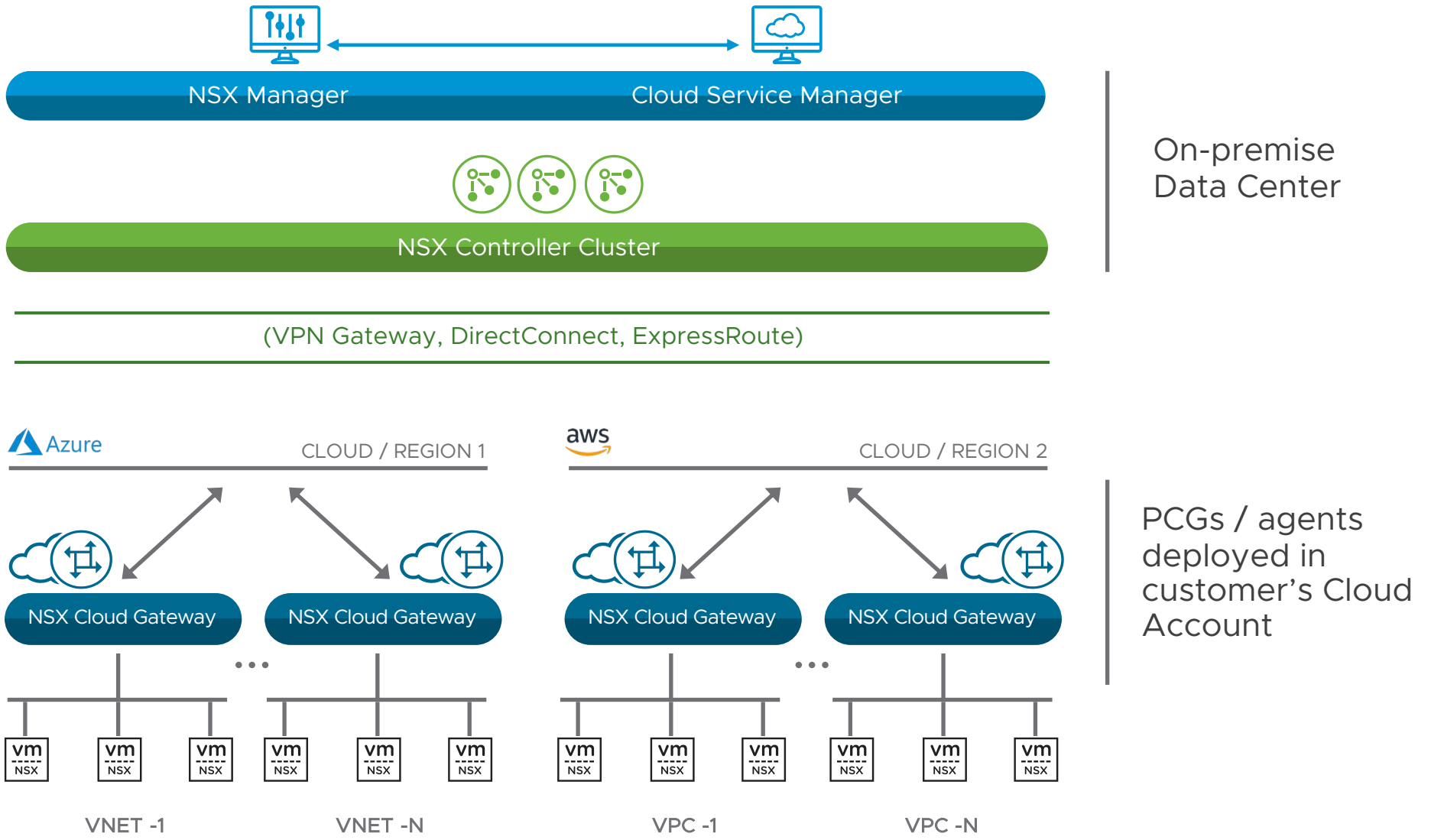
Multi-Cloud Deployment

USDC TECHNOLOGY Smart Data Center

NSX MANAGEMENT PLANE

NSX CONTROL PLANE

CUSTOMER COMPUTE VNET/VPCs



On-premise Data Center

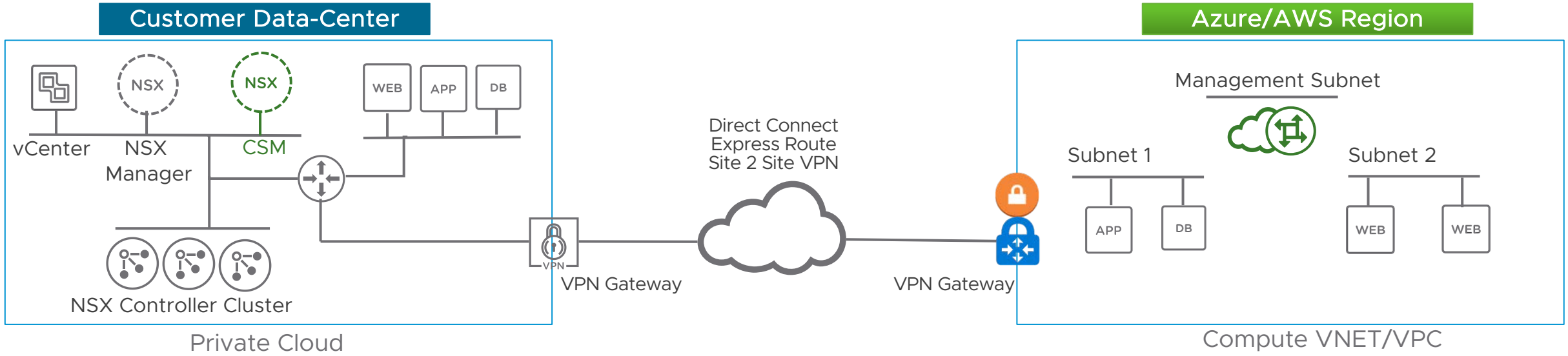
PCGs / agents deployed in customer's Cloud Account

vmware

Common Deployment Topologies

Customer Deployment Architectures – Direct Connections

AWS and Azure

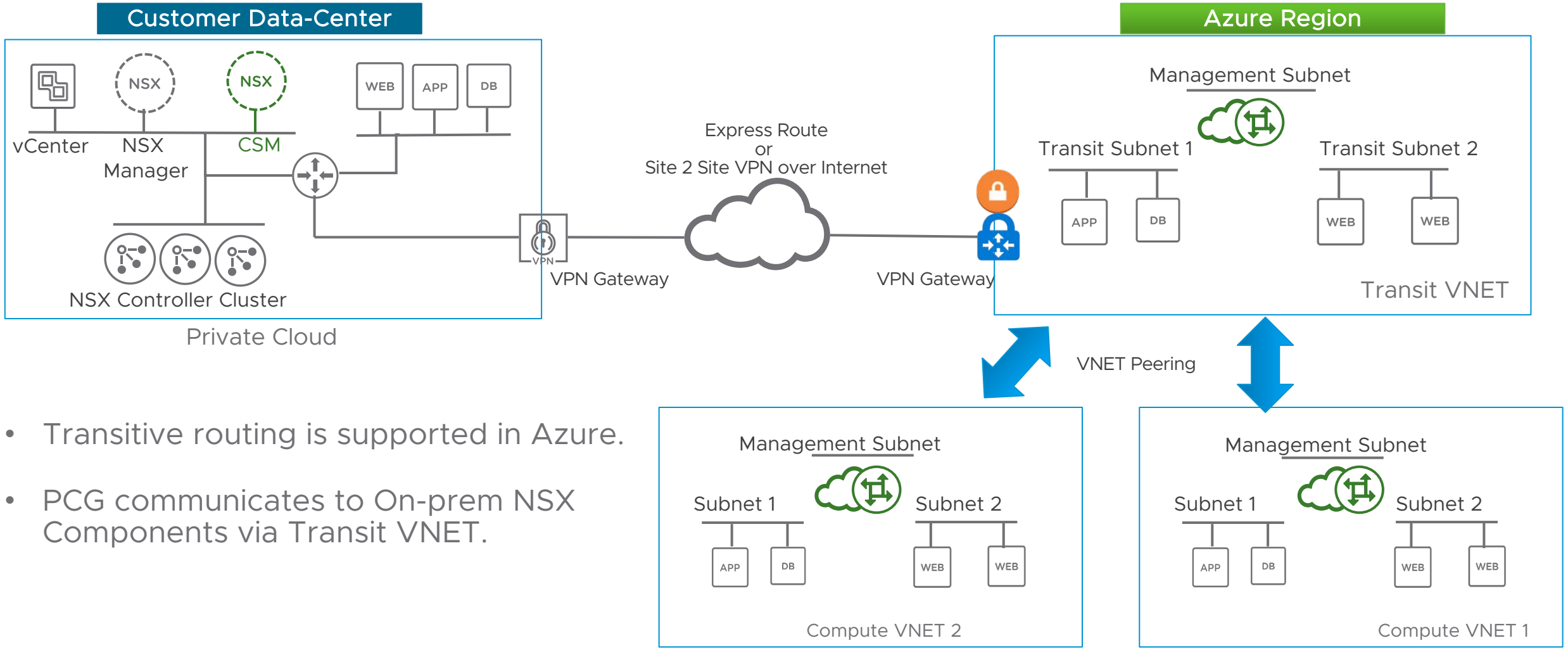


Other considerations

- 150ms round trip between VPC/VNET and on-prem
- Routable IP connectivity between VPC/VNET and on-prem with or without NAT in the path

Customer Deployment Architectures – Transit VNET with Peering

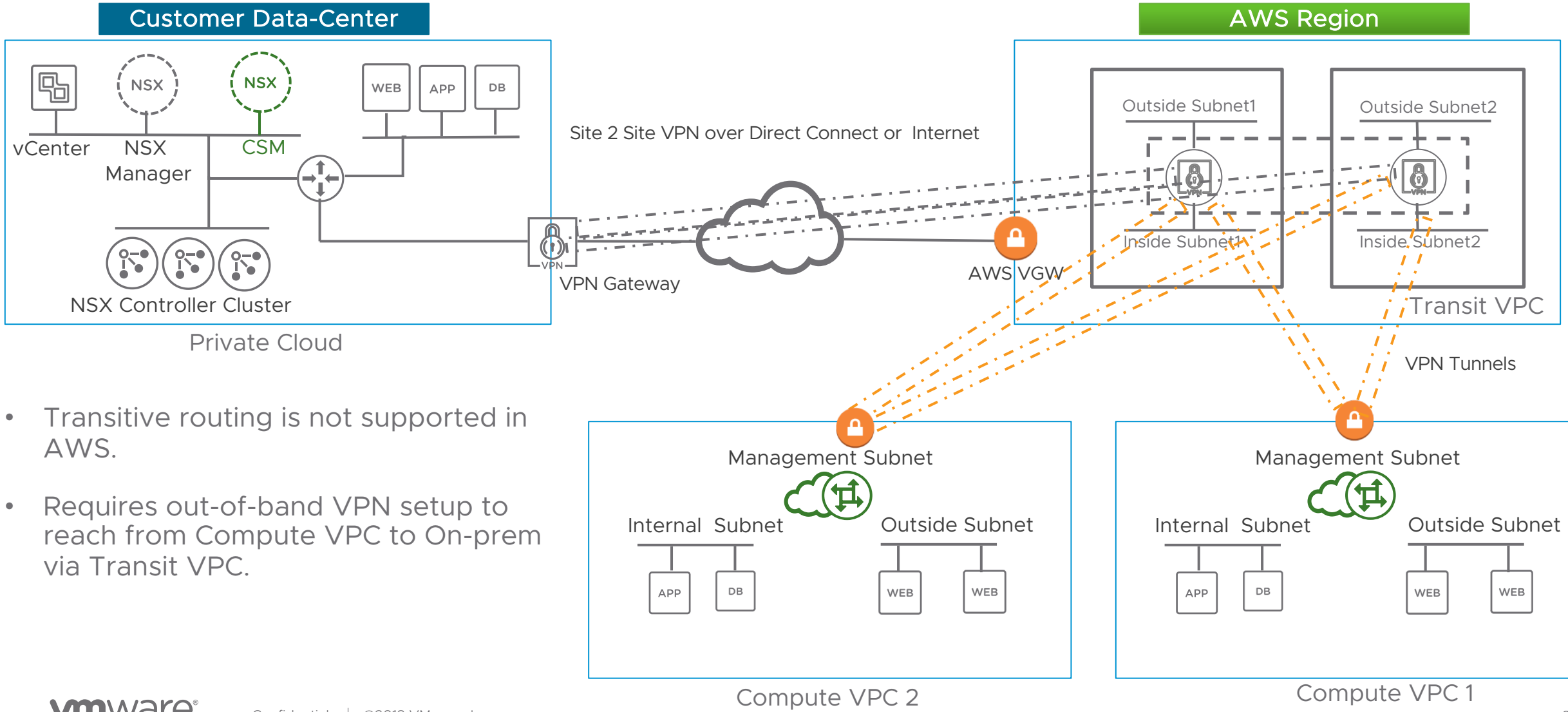
Azure



- Transitive routing is supported in Azure.
- PCG communicates to On-prem NSX Components via Transit VNET.

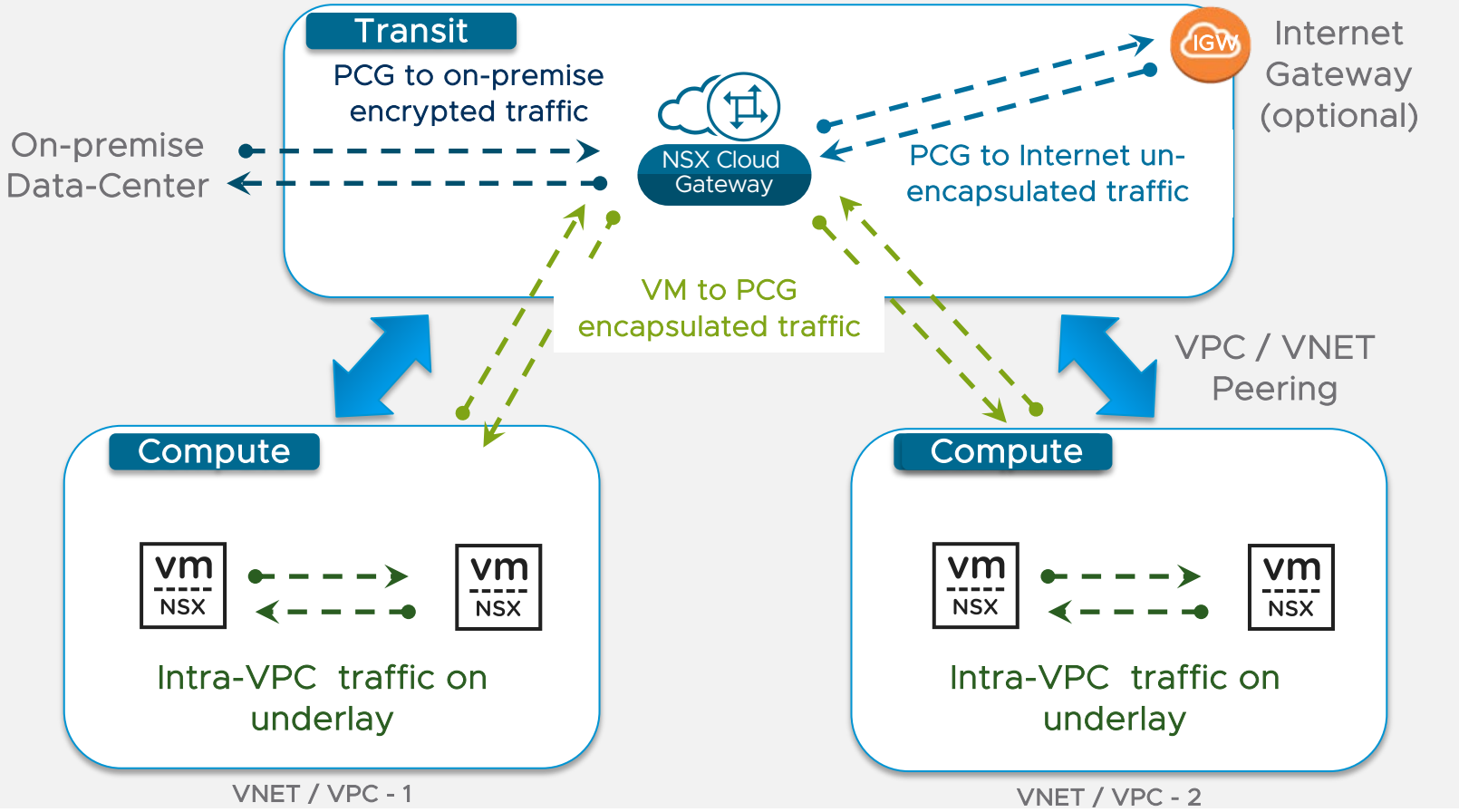
Customer Deployment Architectures – Transit VPC with VPN

AWS



- Transitive routing is not supported in AWS.
- Requires out-of-band VPN setup to reach from Compute VPC to On-prem via Transit VPC.

NSX Cloud Shared Gateway Architecture



- Intra-VPC (VNET) traffic directly on cloud underlay (un-encapsulated)
- Inter-VPC traffic encapsulated in Geneve over peered VPCs/VNETs from each VM to NSX GW
- Destinations external to compute VPC routed via NSX Logical Router

NSX Cloud Summary

Cloud Network Admin

Defines Network Topology & IP addressing

Cloud Security Admin

Mandates security policy and ensures compliance

DevOps / Developer

Focuses on Application development and deployment

Thank You

vmware

USDC TECHNOLOGY
Smart Data Center