Cisco live!

What You Make Possible

TOMORROW starts here.

CISCO

Securing Cloud Security

BRKSEC-2009

Abstract

As the Cloud Compute phenomenon is changing the landscape of IT services with technologies such as virtualisation and multi-tenancy; the fundamental ways to access and use applications as well as data are changing…

> Securing confidential data in accordance with ***regulatory requirements***, fortifying and verifying application software, having ***federated identity management***, and ensuring data is stored and/or maintained in compliance with ***political and legal mandates*** really demands the security professional take a fresh look at the underlying Architectural Principles.
>
> In order to secure data in the Cloud, it becomes necessary to work with the Cloud, not against it.

This session will look at the affects to security policy that Cloud computing introduces, explain new approaches in building secure Cloud Computing architectures and cover some of the new tools and technologies which are used to secure the path to the Cloud.

The target audience for this session are security and data centre administrators. The attendees will also benefit from the following session: BRKSEC-2205 "Security and Virtualisation in the Data Centre”.

Agenda

- What is Cloud?
  - Cloud Security Concerns
- Cloud Security Architectures
  - Securing Cloud Infrastructure
    - Traffic Flows
    - Virtualised Security
    - Extending the Private Cloud into Virtual Private Clouds
  - Securing Cloud Security Services
- Summary

What is Cloud?

The Meaning of Cloud

What? Essential Characteristics (NIST)

- Self Service
- Broad Access
- Resource Pooling
- Rapid Elasticity
- Measured Services

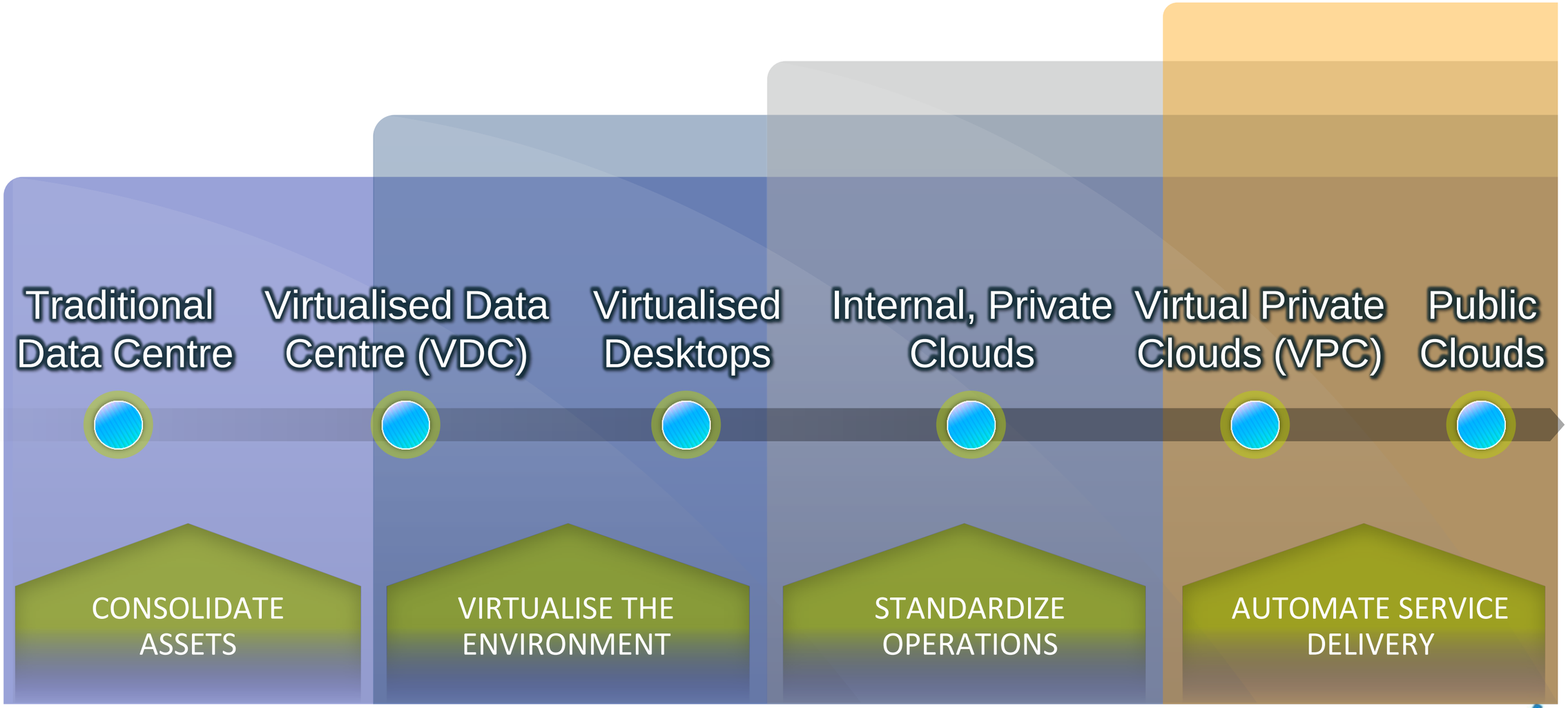
How? Service Models

- IaaS — VM
- PaaS — VM, OS, FRAMEWORK
- SaaS — APPLICATION

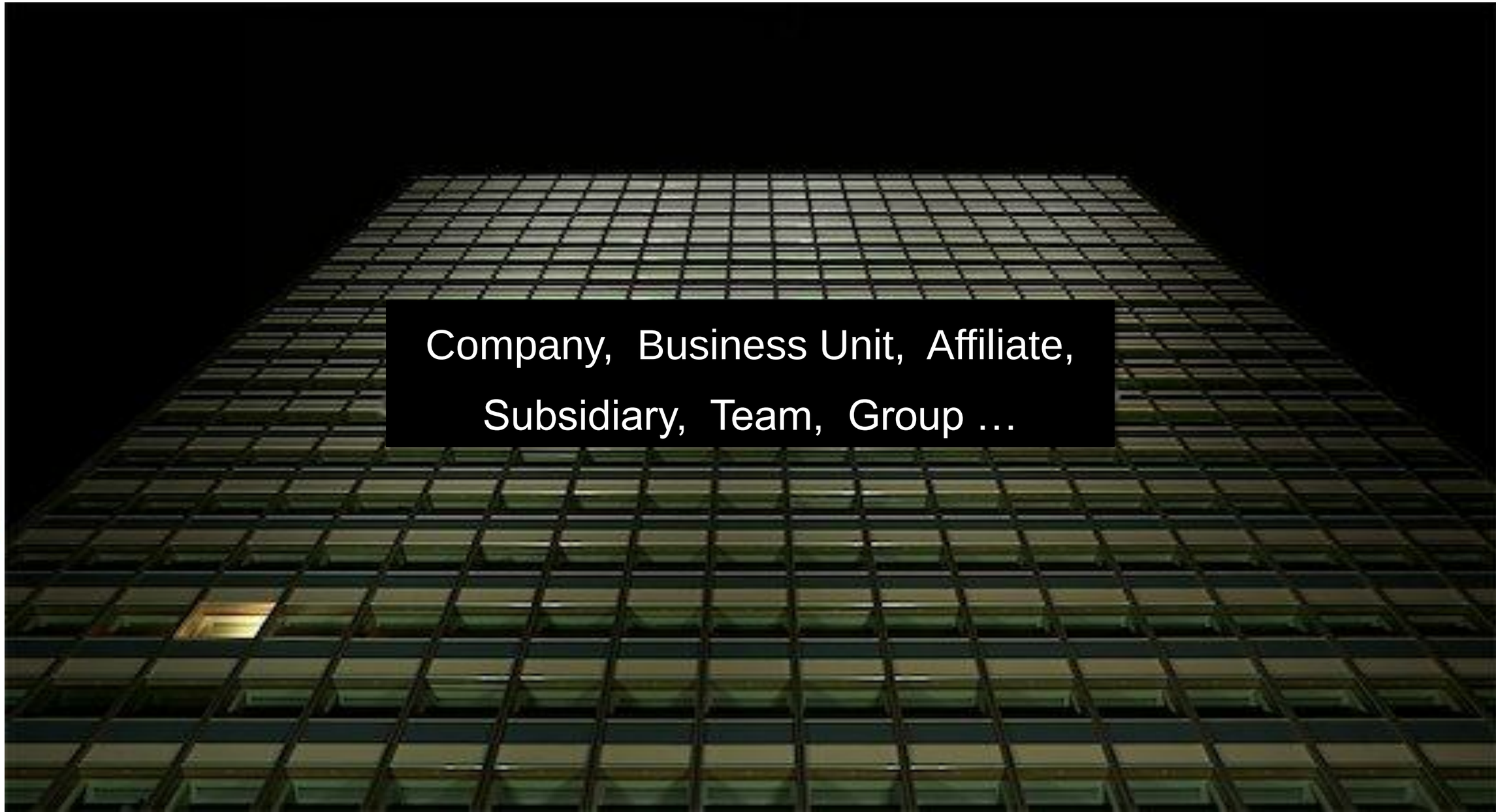
Where? Deployment Models

- Private
- Community
- Virtual Private
- Hybrid
- Public

The Cloud Journey



Multitenancy: You are not alone…



Cloud Security Concerns

Cloud is Happening…

With or Without Security

Cloud Security Concerns

Management

Information Security

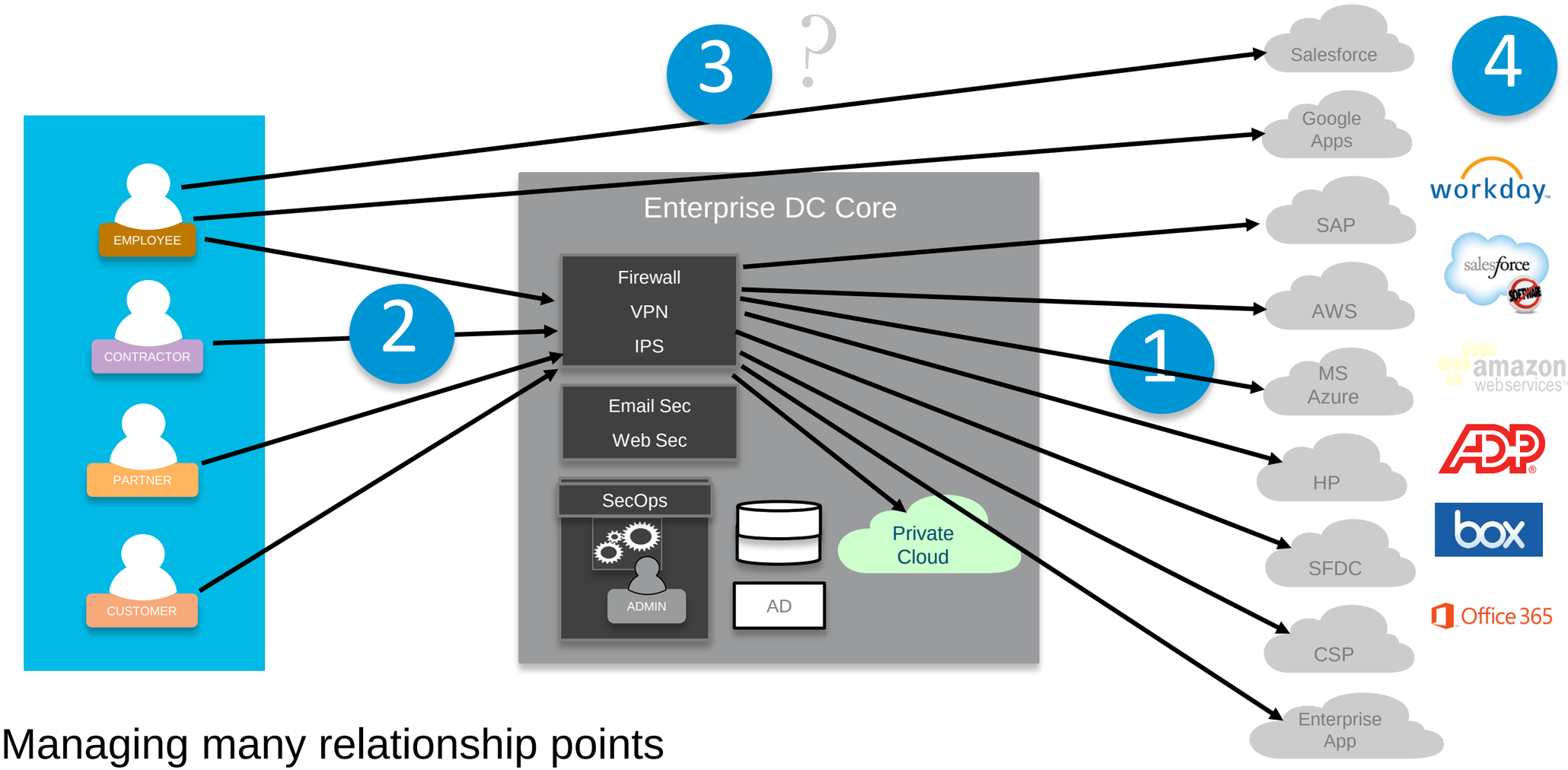
- Company/tenant data isolation
- Data-at-rest and Data-in-Flight

Access to data and applications

- Identity and authorisation
- Local and remote access

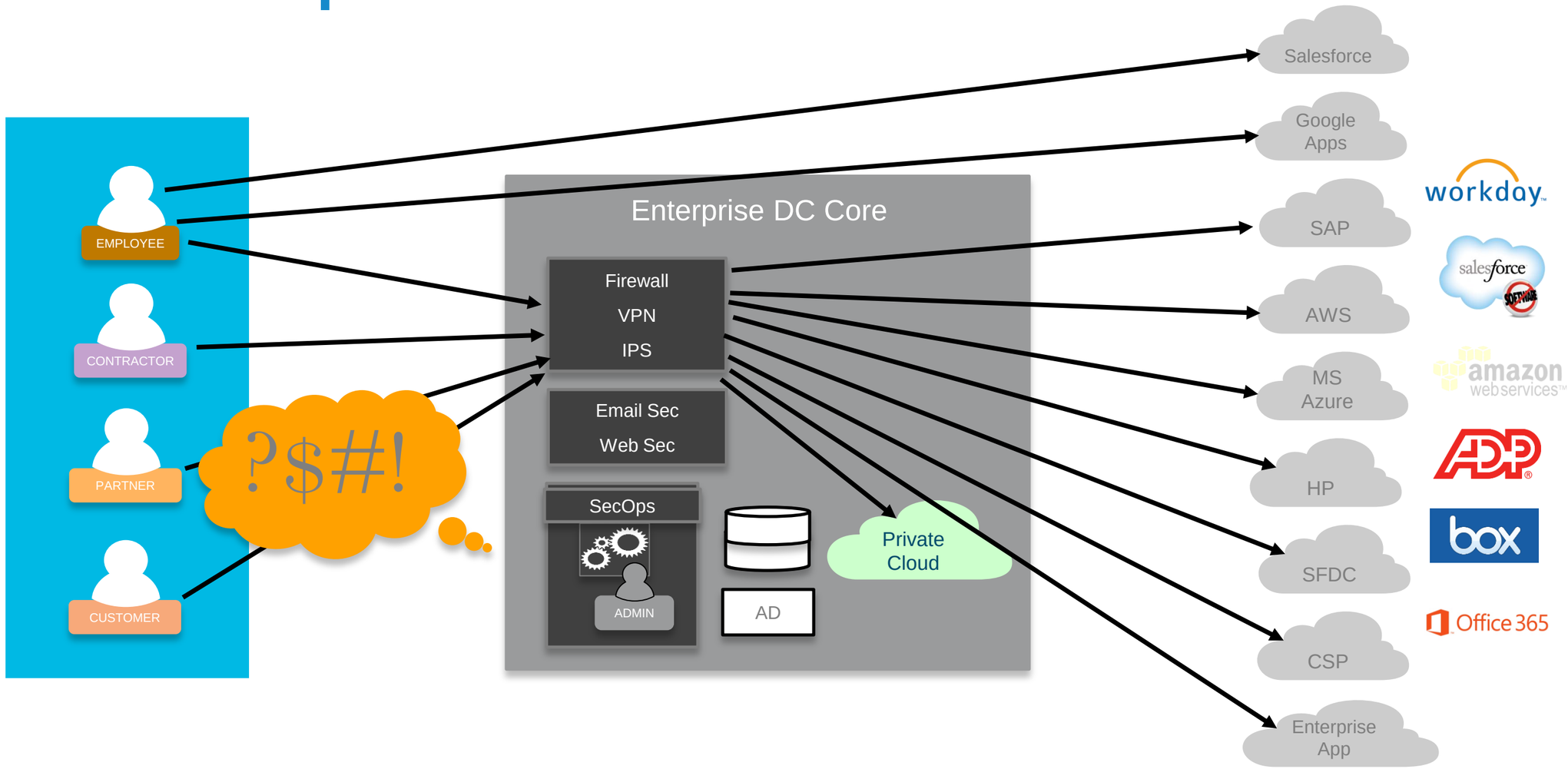
- Loss of control & visibility
- System complexity & multi-teams
- Compliance

Current Multiple Cloud Provide Environment



1. Managing many relationship points
2. Access to cloud applications is concentrated through the datacentre
3. Cloud applications activity blindness
4. InfoSec scare: “Oh ****, our data is in the cloud, is it hackable?”

Current Multiple Cloud Provide Environment



How to have visibility, and control access, applications, and data in the cloud?

Cloud Security Architectures

The Security Policy

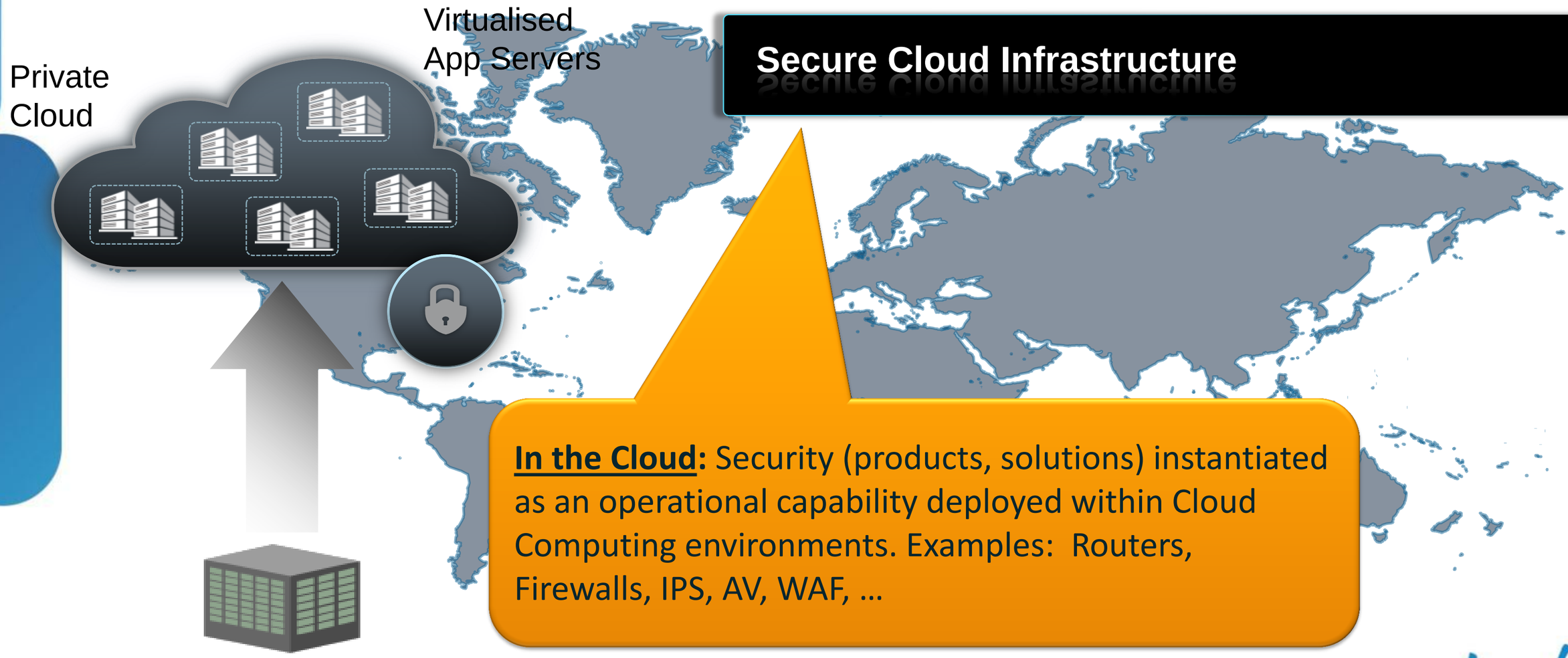
- Wikipedia: “Security policy is a definition of what it means to be secure for a system, organisation or other entity.
  - For an organisation, it addresses the constraints on behaviour of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls.
  - For systems, the security policy addresses constraints on functio and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.”
- It is NOT acceptable to implement virtualisation or Cloud technologies in such a manner that the System is no longer compliant with the Security Policy

Architectural Requirements

- Logical separation
- Policy consistency
- Authentication and access control
- Scalability and performance
- Automation

Cloud Security: Defined

"In the Cloud"



Cloud Security: Defined

"For the Cloud"

Secure Cloud Infrastructure

Secure Cloud Access

For the Cloud: Security services that are specifically targeted toward securing OTHER Cloud Computing services, delivered by Cloud Computing providers.

Cloud Security: Defined

"By the Cloud"

Secure Cloud Infrastructure

Securing Cloud Access

Cloud Security Services

By the Cloud: Security services delivered by Cloud Computing services which are used by providers

Securing Cloud Infrastructure

Cloud Infrastructure Security

- Traditional Security Problems Persist

  Physical security, L2/L3 security, DDoS protection, etc…

- Security Policies still need to be enforced, <u>regardless of physical/virtual location of the resource being protected!</u>
- Virtualisation introduces some new flavors
  - Hypervisor is a new layer of privileged software
  - Potential loss of separation of duties
  - Limited visibility into inter-VM traffic

Security Best Practices

- Physical Security
- Network Infrastructure
  - Layer 2/Layer 3 Security
  - Router/Switch hardening
  - Control Plane Policing
  - DDoS protection
  - High Availability (HA)
  - Application Security at NW layer
  - Operational Security at NW layer
  - Monitoring & Assurance
- Application Infrastructure
  - Hypervisor protection
  - VM protection
  - OS protection
  - Patch maintenance and updates
  - Monitoring and Assurance
- Management Infrastructure
  - Dedicated zones/VMs
  - Dedicated NW
  - Operator Access control
  - Failover mechanism

Cisco Virtualised Multiservice Data Center - VMDC

Reference Architecture for Secure DC Design

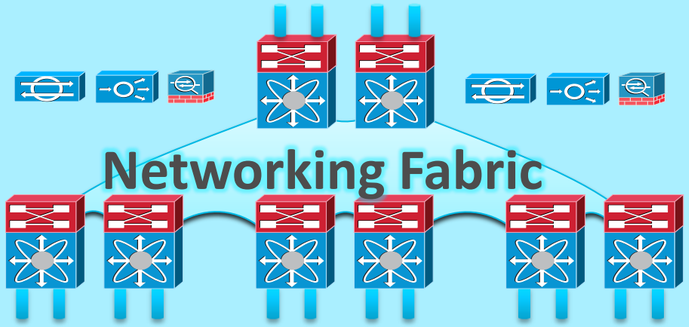
Inter-Data Centre Networking

WAN

Multi-Site Connectivity

Unified Fabric and Data Centre Networking

Providing Network and Services Virtualisation



Networking Fabric

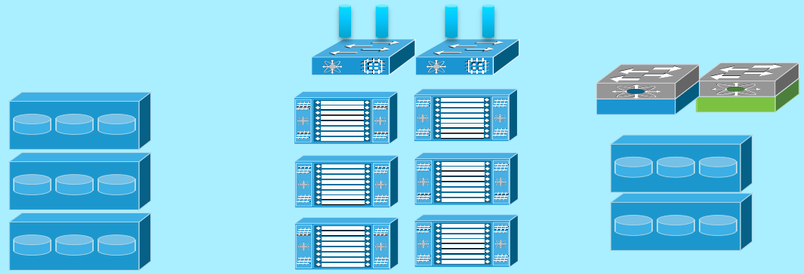
Services

Network Fabric

Unified Computing and Integrated Systems

Providing Server and Application Virtualisation

Unified Computing



NAS

Compute

SAN

Access

Storage

Compute

Cloud Service Management

- Business Support
- Provisioning Configuration
- Portability/ Interoperability

VMDC

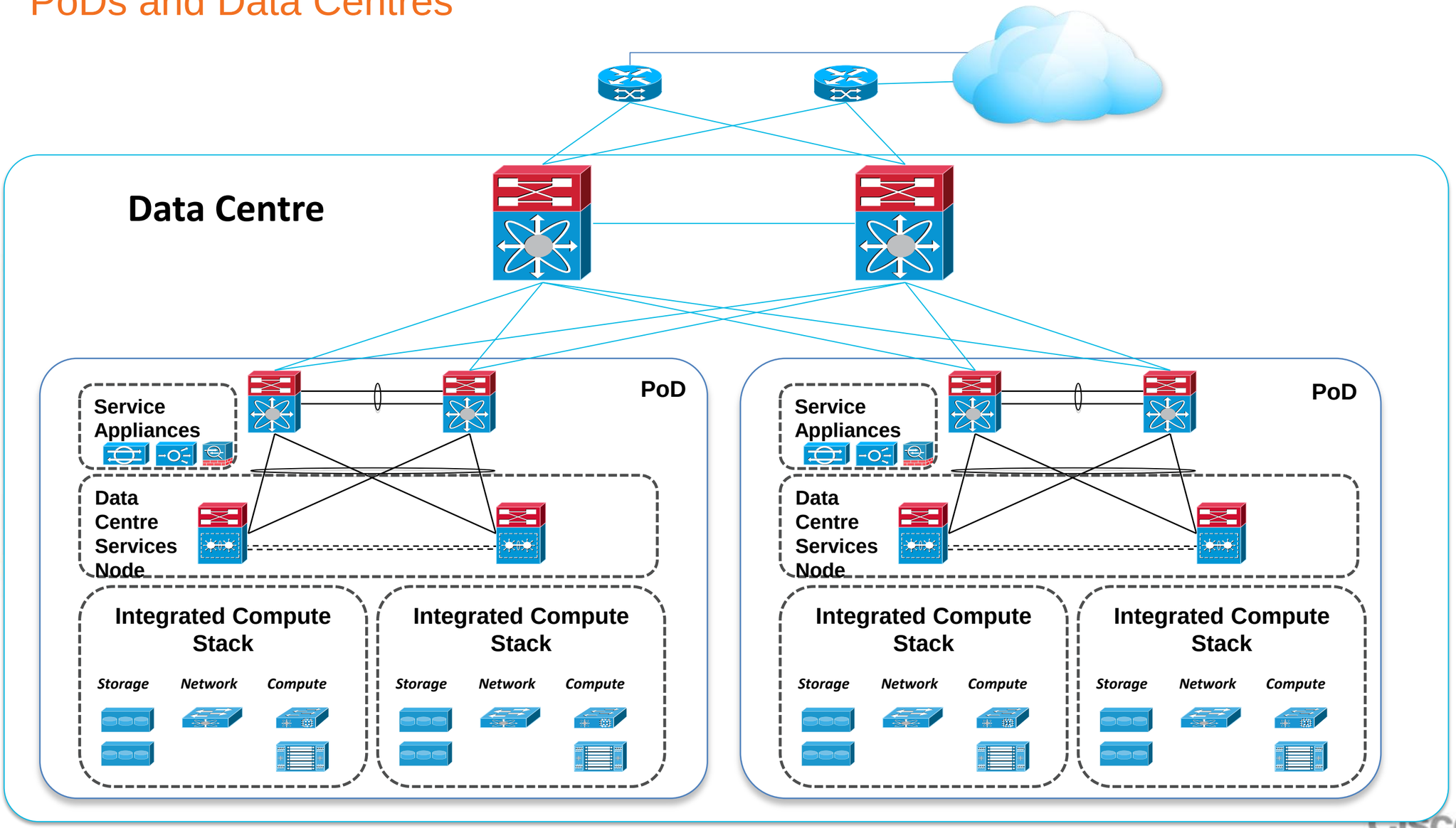
Secure DC Design Highlights in VMDC

- Secure Infrastructure Design:
  - Secure multi-tenancy
  - High Availability
  - Differentiated Services
  - Role Based Access Control
- Business Continuity and Disaster Recovery
- Monitoring and Assurance
- Hardening through test and Validation

- Orchestration and Automation validated over VMDC
  - BMC CLM
  - Cisco IAC and NSM
  - Citric CloudStac
- Applications validated over VMDC
  - HCS
  - VXI
  - Telepresence
  - Etc.

Basic VMDC Building Blocks

PoDs and Data Centres

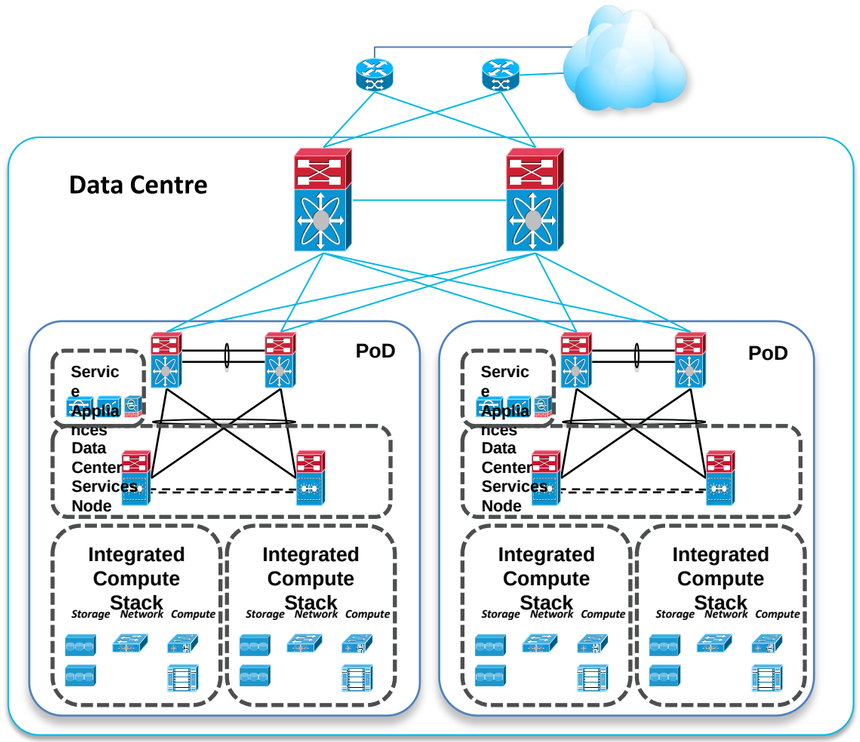


Basic VMDC Building Blocks

PoDs and Data Centres

Key Design Considerations:

- L2 Scale - Virtual Machine Density, VMNics per VM, MAC Address Capacity, Cluster Scale, ARP Table Size, VLAN scale, Port Capacity, Logical Failure Domains, L2 Control Plane
- L3 Scale – BGP Peering, HRSP Interfaces, VRF Instances, Routing Tables and Convergence, Services
- Resource Oversubscription – Network Compute, and Storage Oversubscription, Bandwidth per VM

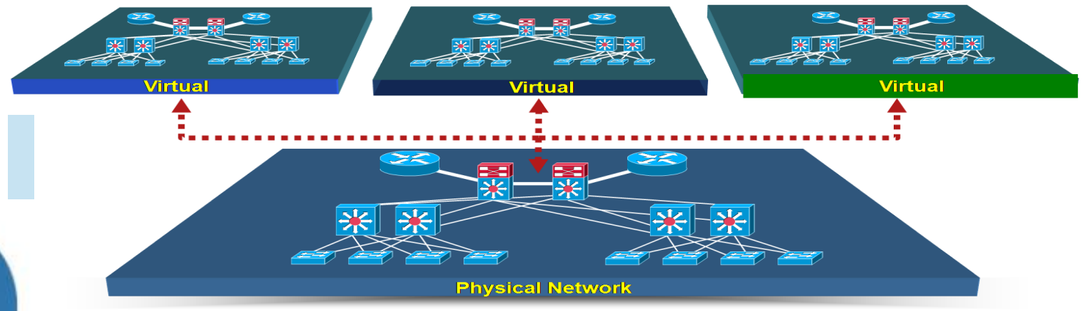


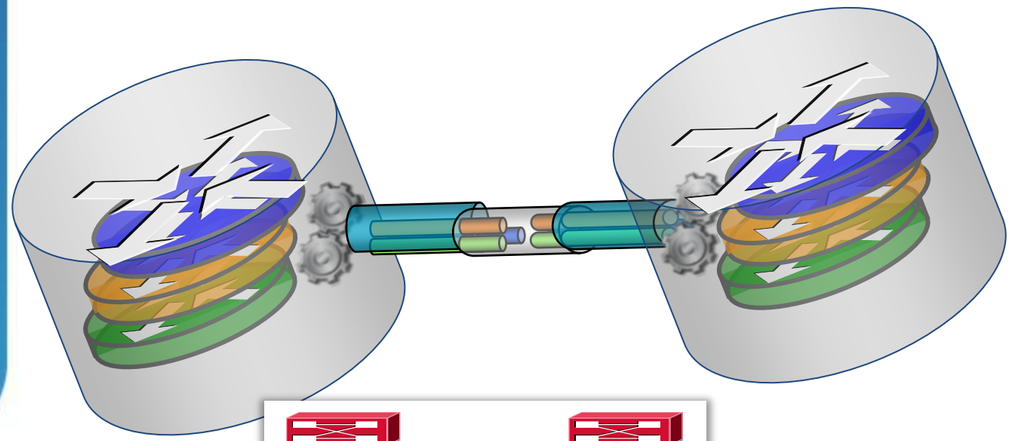
How to Design a Tenancy Container

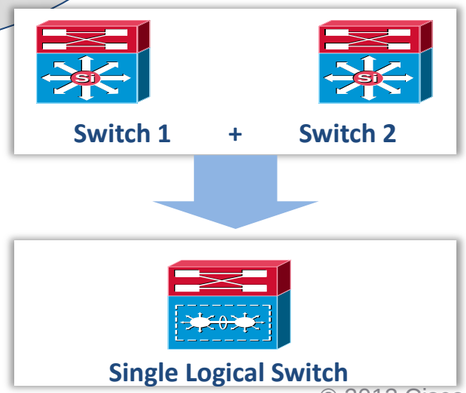
- What is your Organisation's Security Policy?
- What is to be hosted in a tenant container
  - Applications
  - Multiple applications
  - Users
  - Mix
- Security zones
  - Shared zones: DMZ, shared public zone for internet access
  - Zones inside a container:
- Size matters

Multi-Tenancy

Techniques used to provide separation



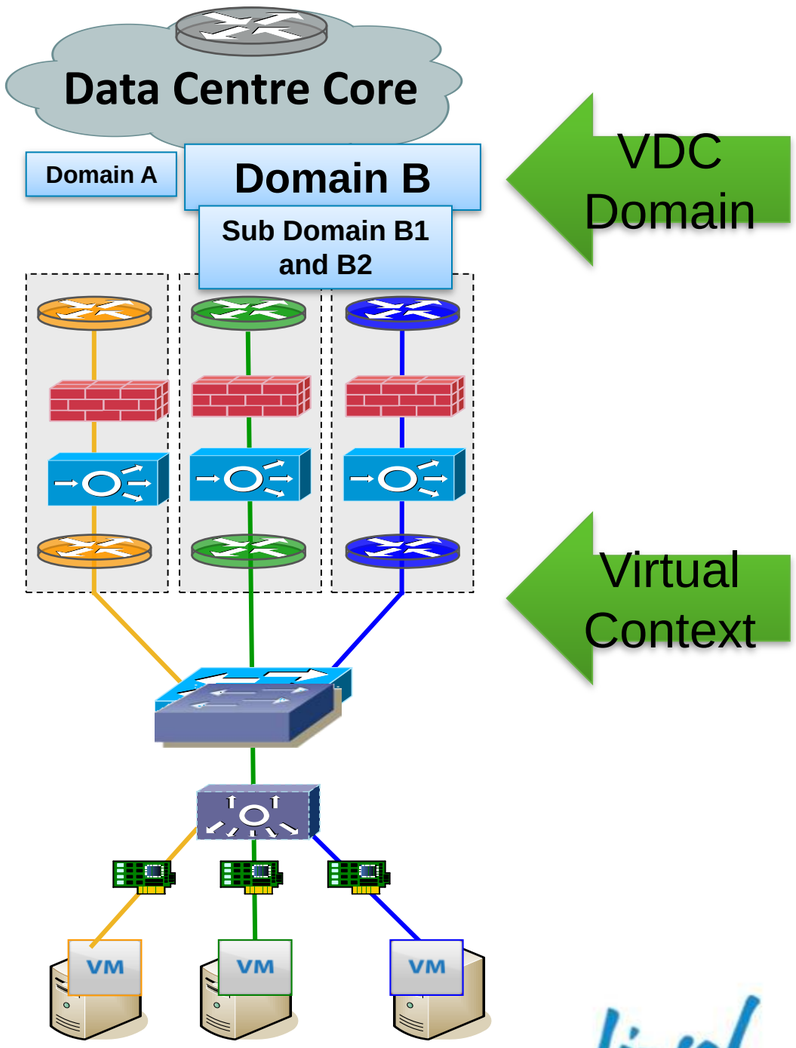




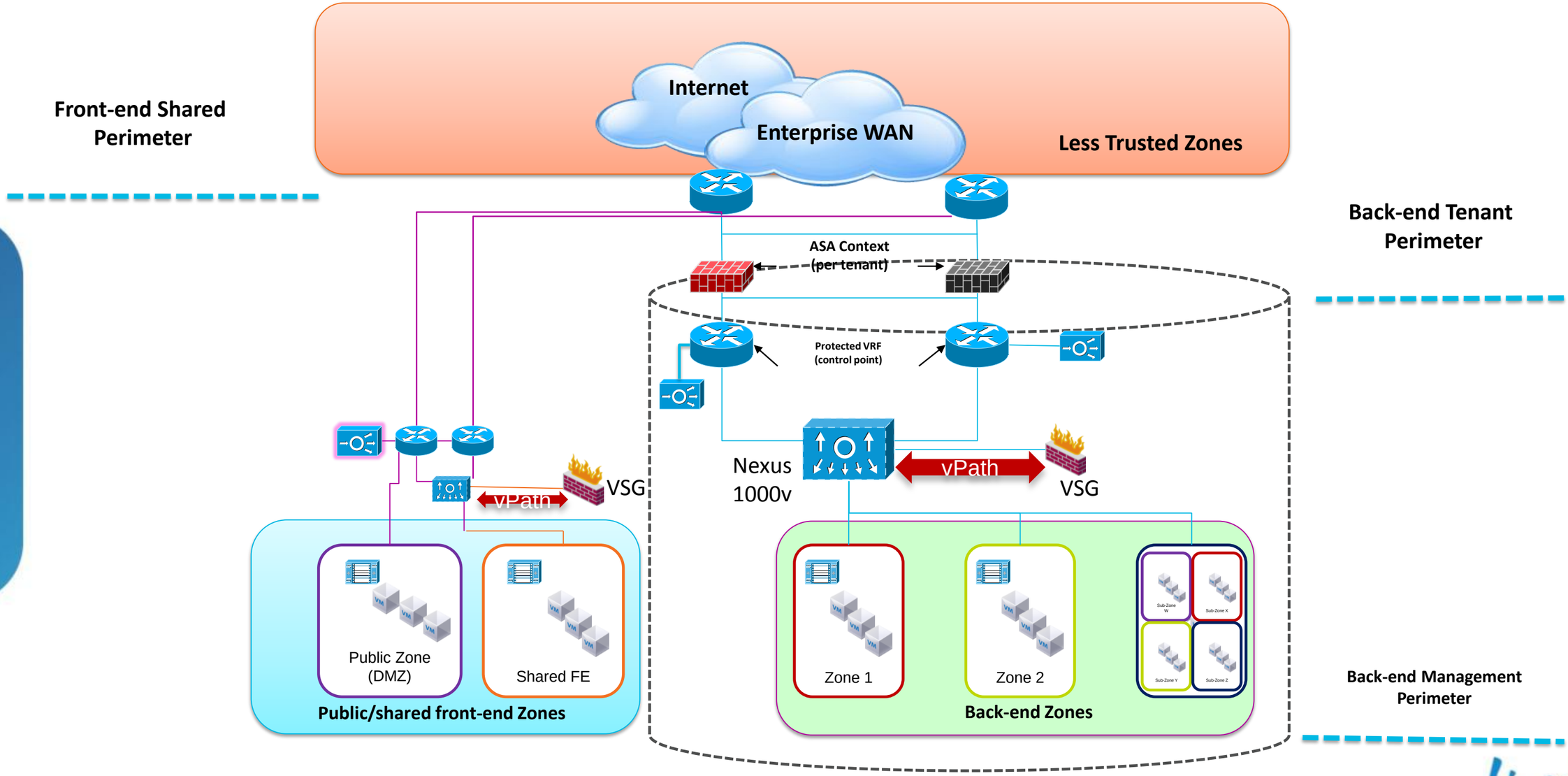
- Device Partitioning
  - One to many devices
  - Primary use case is infrastructure reduction
  - Increases service agility, flexibility and asset utilisation
  - Examples: VLAN, VRF, VSAN, VDC, Firewall Context, LB Context, Hypervisor
- Virtualised Interconnect
  - Multiple “wires” within a wire
  - Primary use case is link consolidation
  - Logical Tennant isolation
  - Examples: 802.1q, VPN, MPLS, Unified I/O FCoE, VXLAN, VN-Link
- Device Pooling
  - Many to one device
  - Primary use case is maximum availability & density
  - Reduces management plane
  - Examples: VSS, vPC, GSLB, FHRP

Creating Tenant Based Segmentation

- Baseline with VLAN, PVLAN, ACL segmentation, and service integration
- Use segmentation to map security domains to each tenant and separate compliant and non-compliant systems.
- Device virtualisation can be leveraged to segment traffic flows and provide insertion points for application and security services
  - Goes beyond VLAN segmentation by separating device management, control, and data planes.
  - Unique policies and traffic decisions can be applied to each context creating very flexible designs



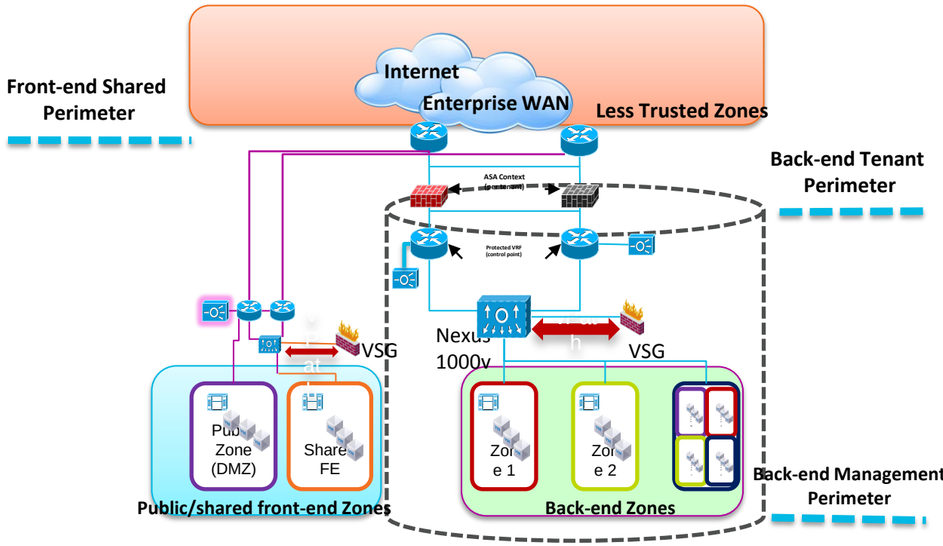
VMDC Consumer Model Example



VMDC Consumer Model Example

Design Considerations:

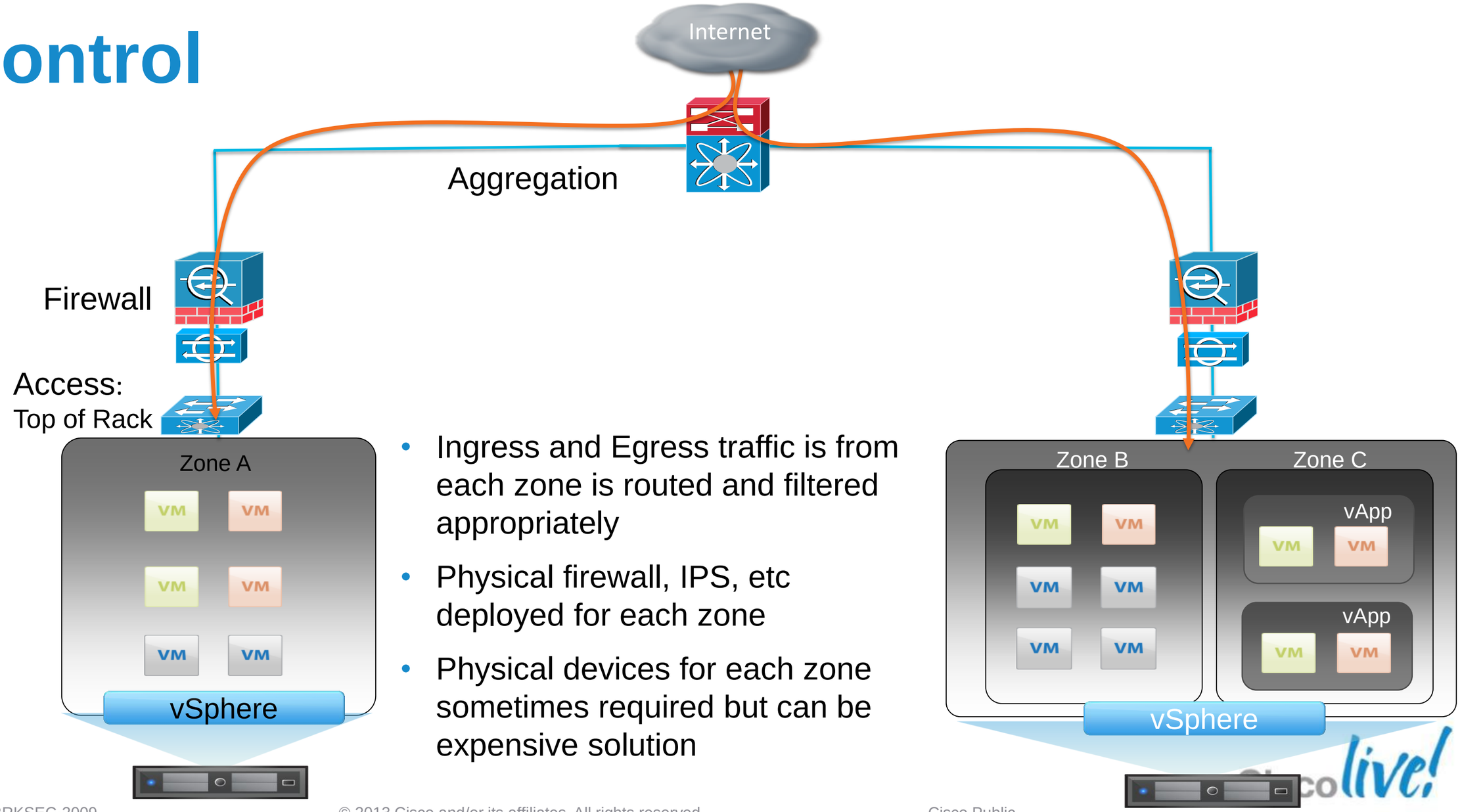
- Baseline: Use logical segmentation (VLAN, ACLs, PVLANs, VRFs) to map security domains to each consumer, separating compliant from non-compliant systems.
- For Public Cloud, separate front-end Private and Public VRFs
- Protected VRF for Layer 3 services, Default gateway for virtual machines
- Dedicated ASA virtual firewall context to enforce stateful security services on ingress and egress data centre tenant traffic
- Allow for zoning
- VSG security services applied across the virtual compute layer to enforce VM security policies



Securing Cloud Infrastructure

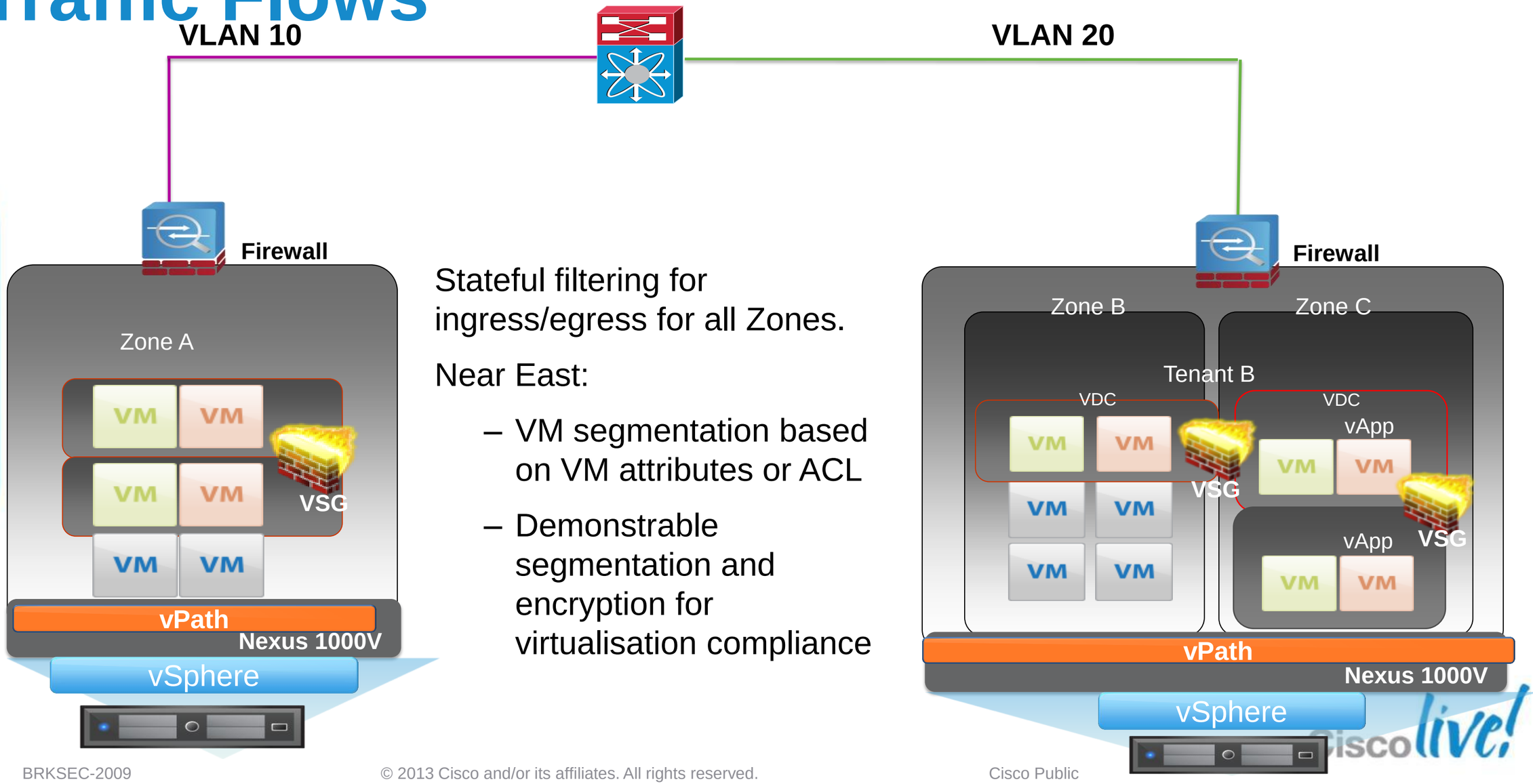
Traffic flows

Traditional North-South Traffic Flow Control



- Ingress and Egress traffic is from each zone is routed and filtered appropriately
- Physical firewall, IPS, etc deployed for each zone
- Physical devices for each zone sometimes required but can be expensive solution

Microsegmentation for East-West Traffic Flows

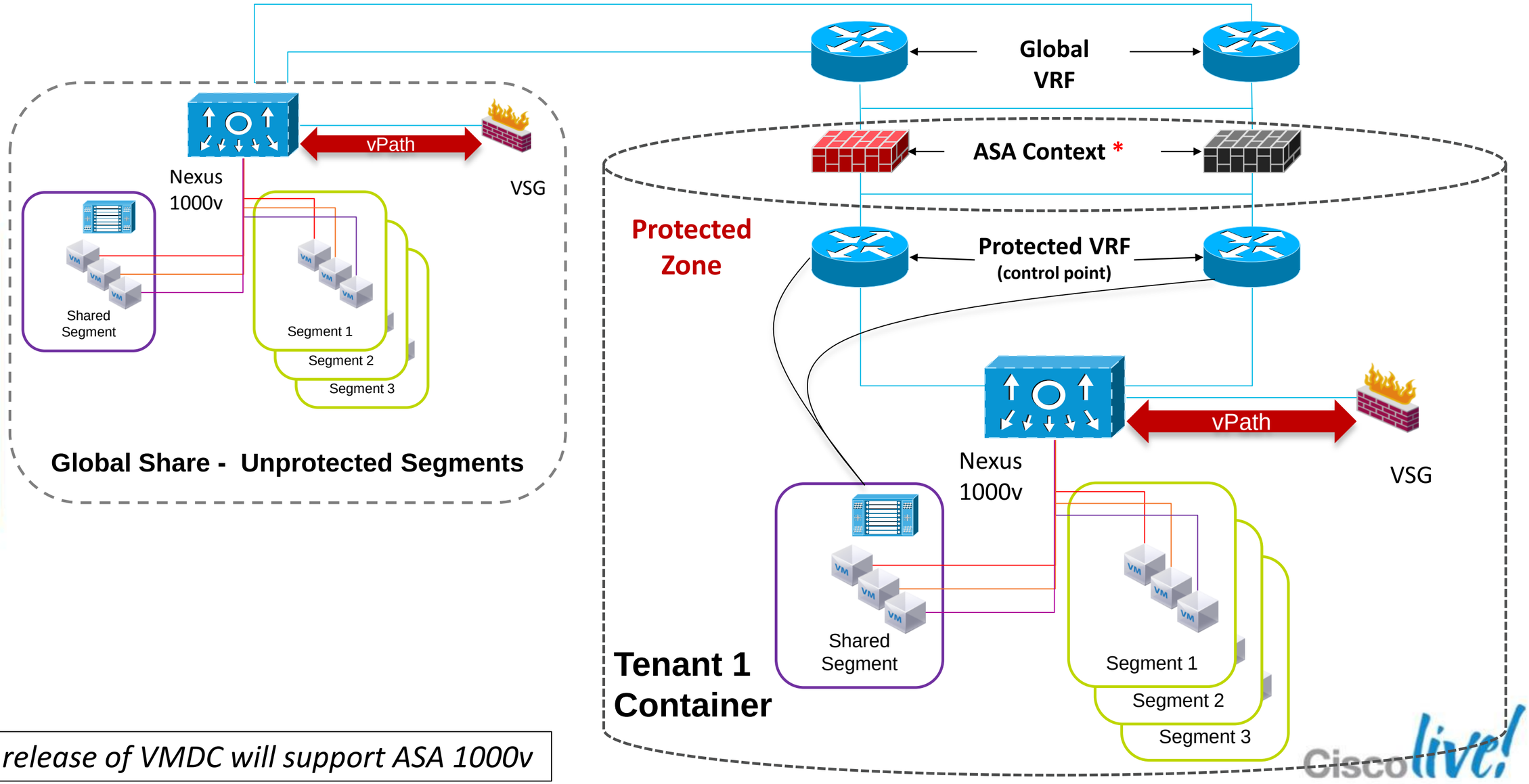


Stateful filtering for ingress/egress for all Zones.

Near East:

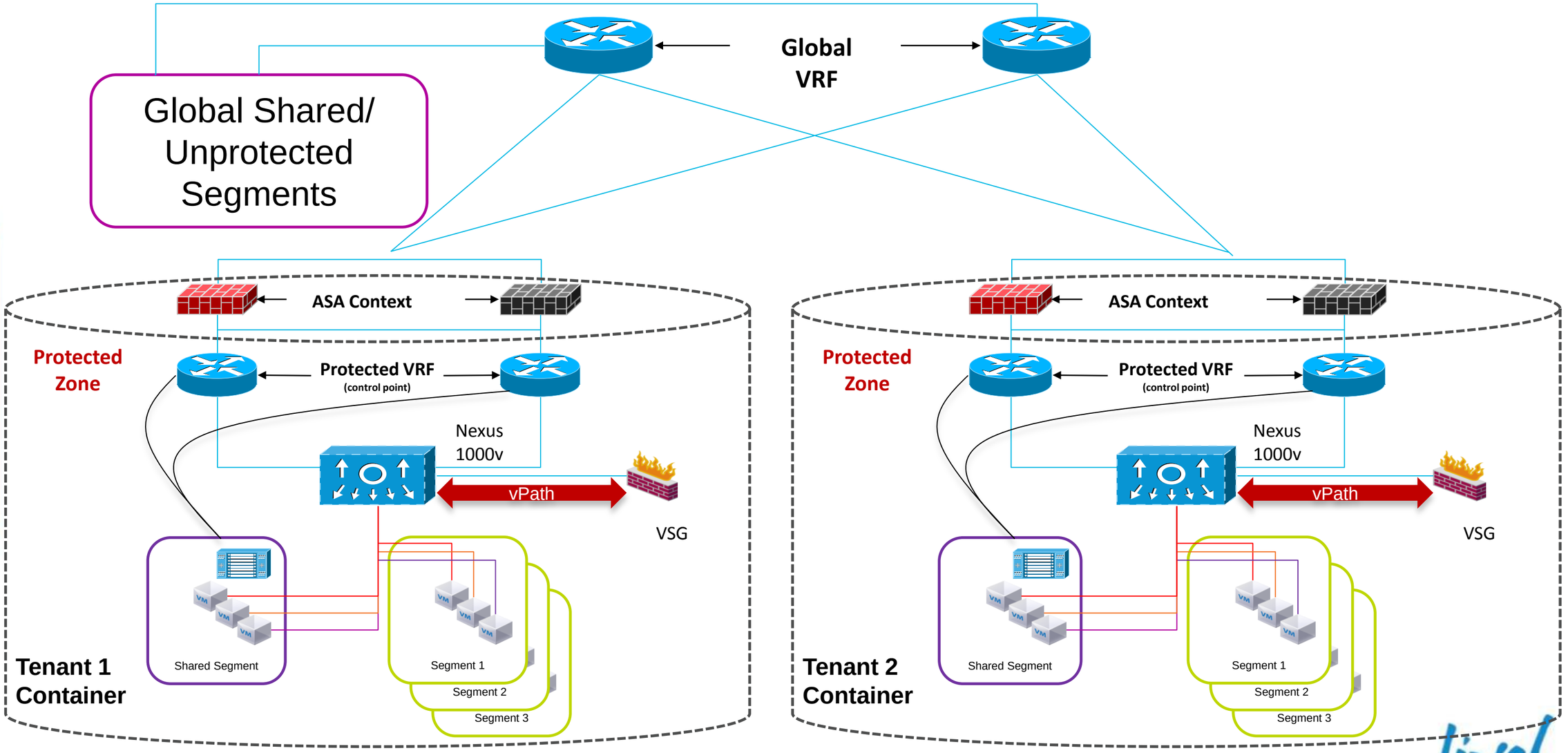
- VM segmentation based on VM attributes or ACL
- Demonstrable segmentation and encryption for virtualisation compliance

VMDC Single Tenant Foundational Model

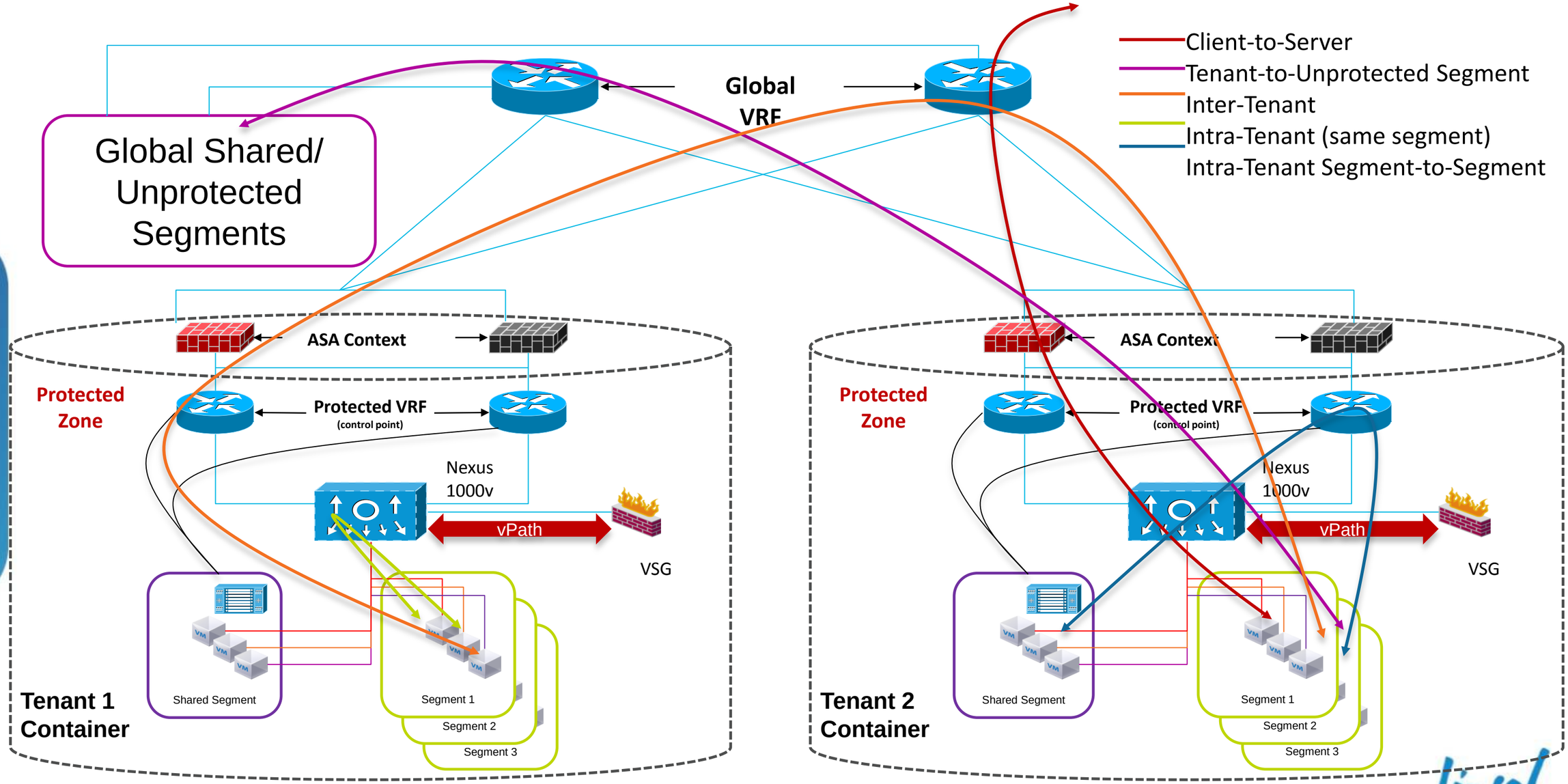


* *Next release of VMDC will support ASA 1000v*

Extending the Single Tenant Model to Multiple Tenants

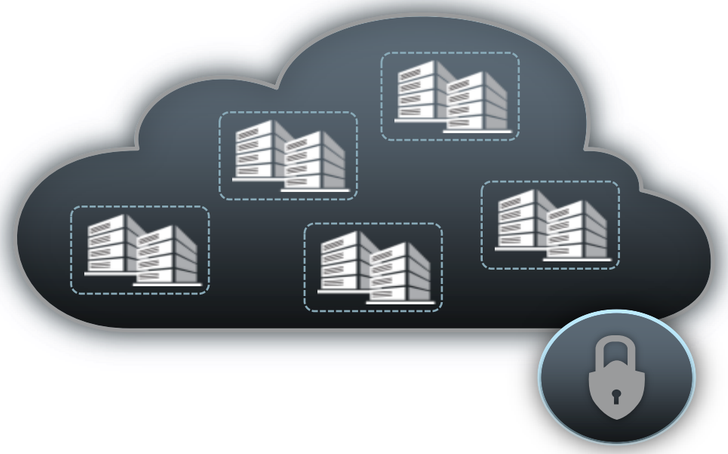


VMDC: Traffic Patterns

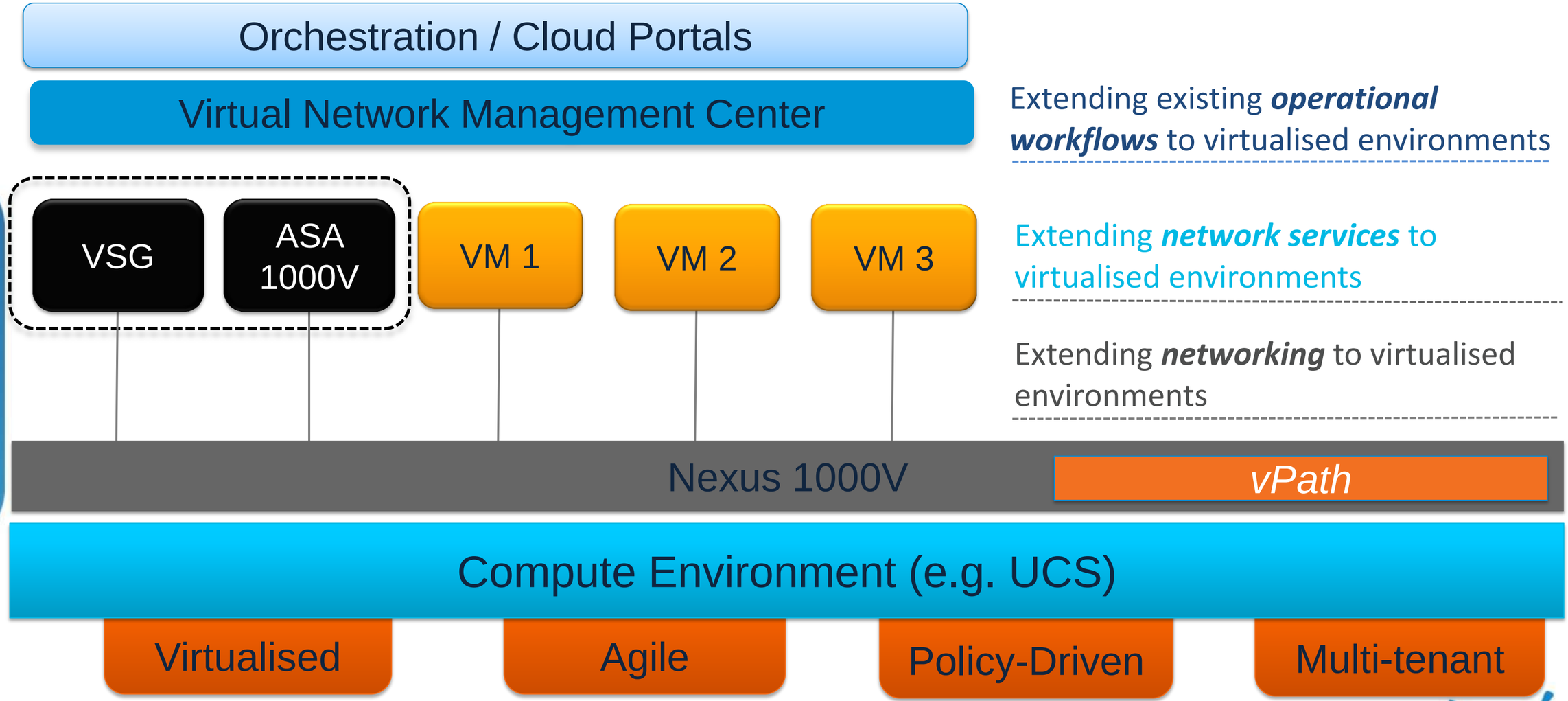


Securing Cloud Infrastructure

Virtualised Security



Cisco's Virtual Security Architecture

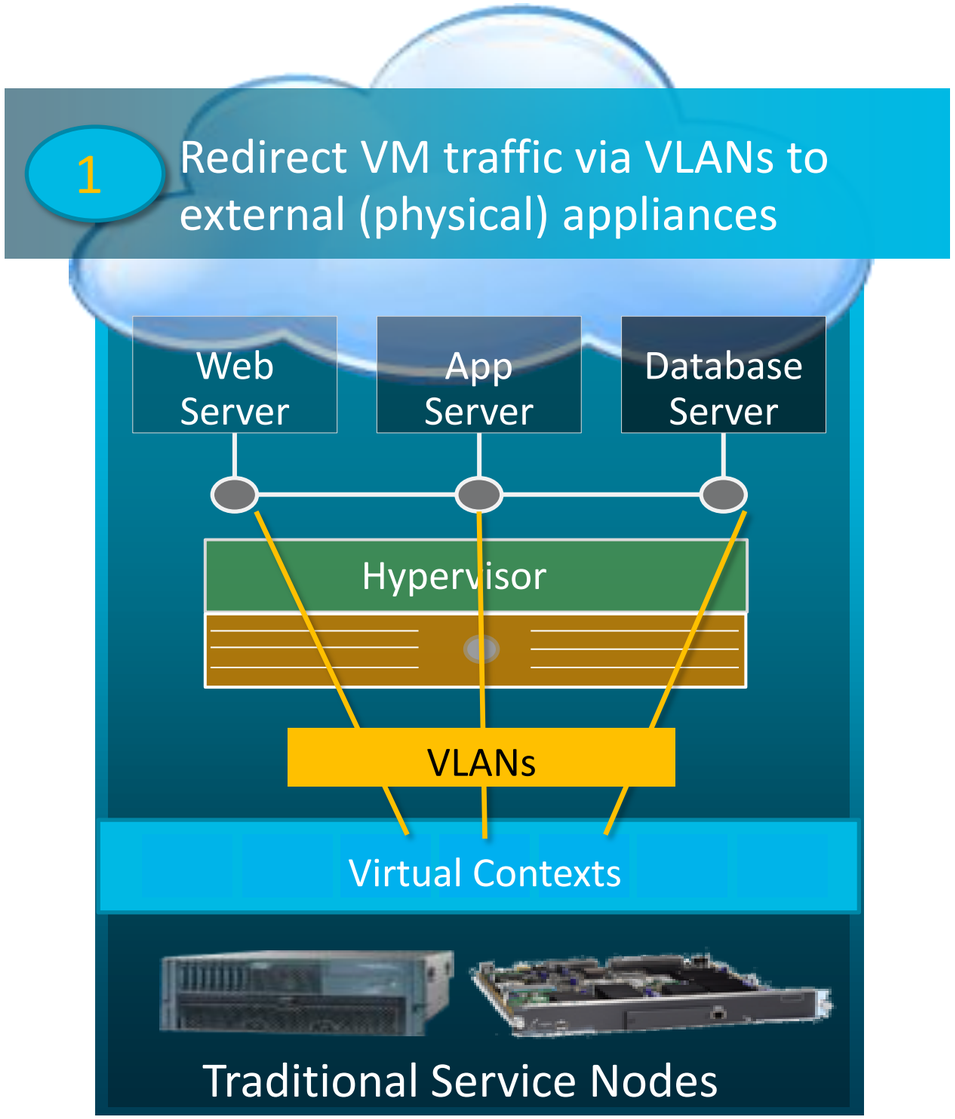


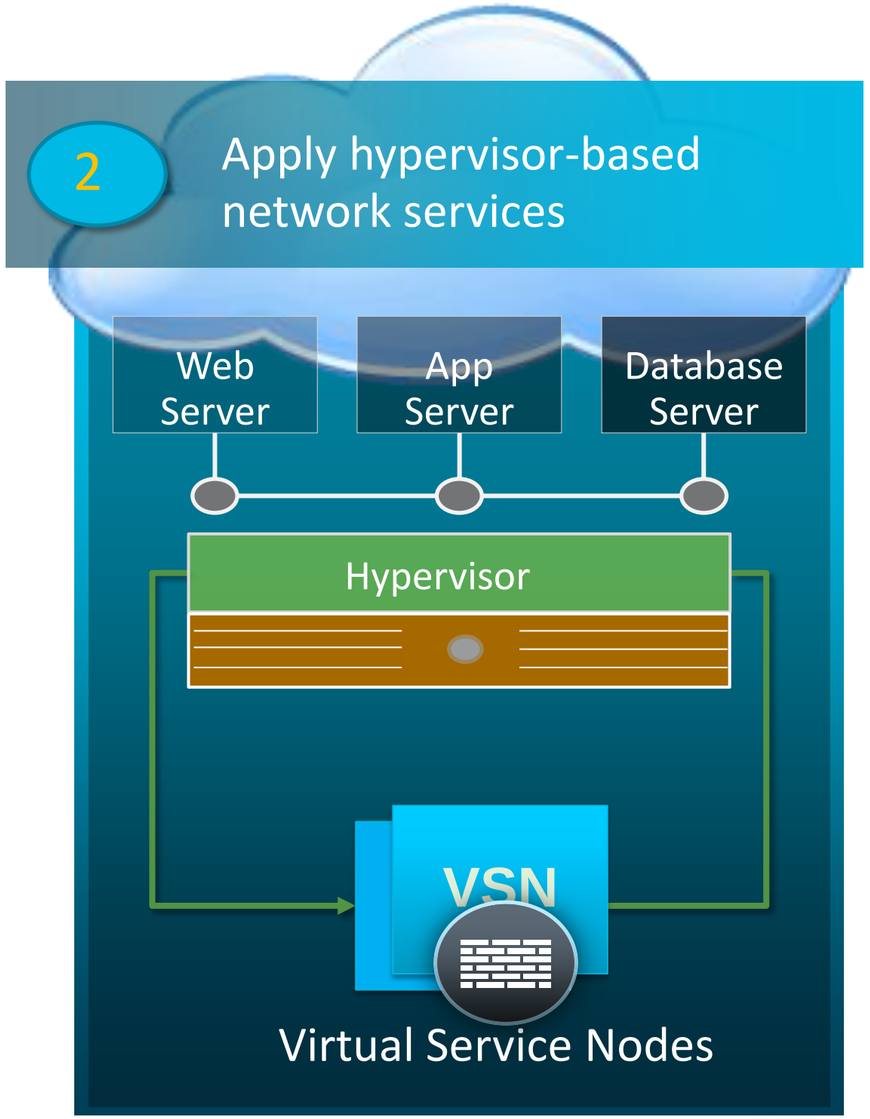
Extending existing ***operational workflows*** to virtualised environments

Extending ***network services*** to virtualised environments

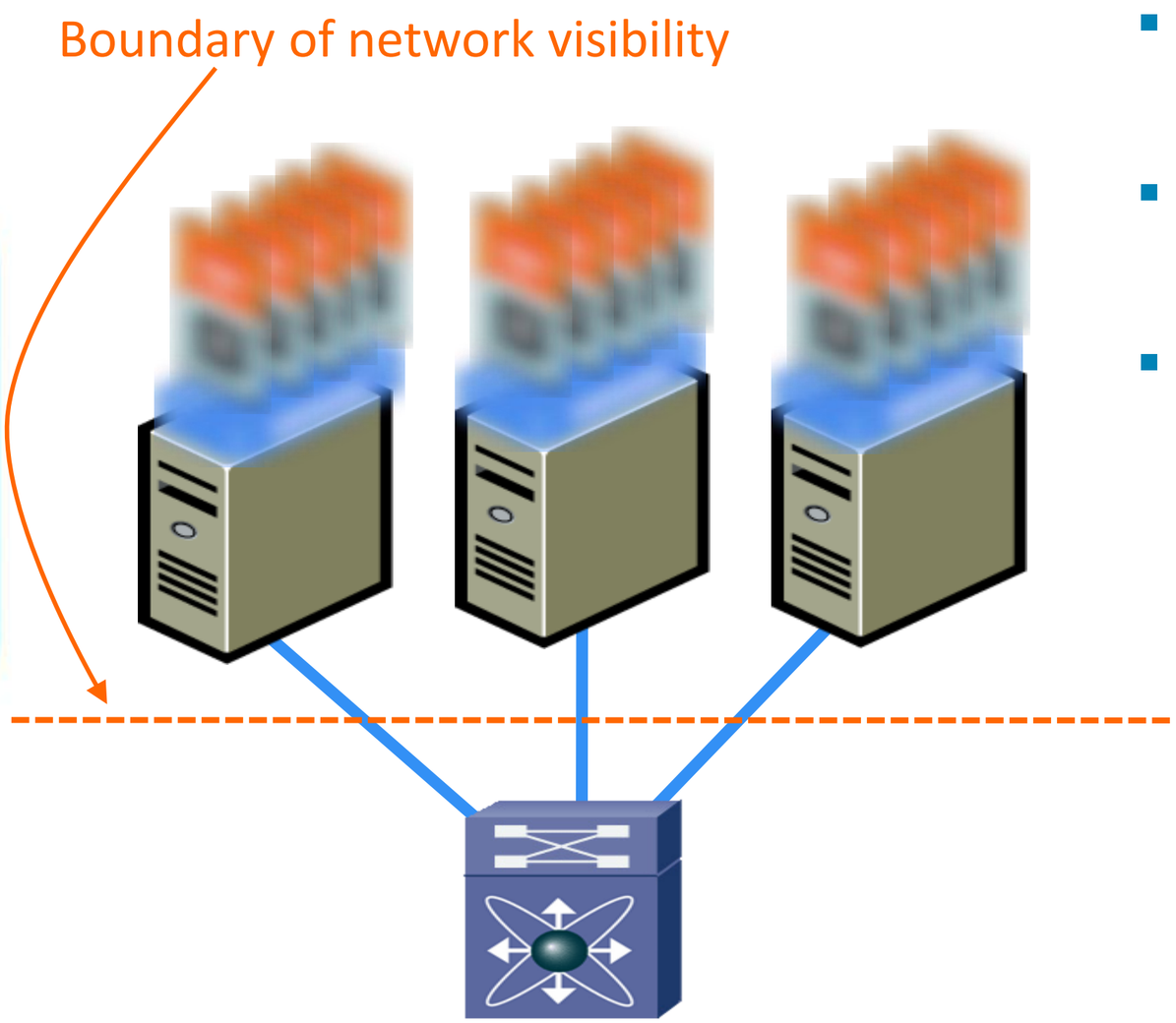
Extending ***networking*** to virtualised environments

Services – Virtual Service Nodes



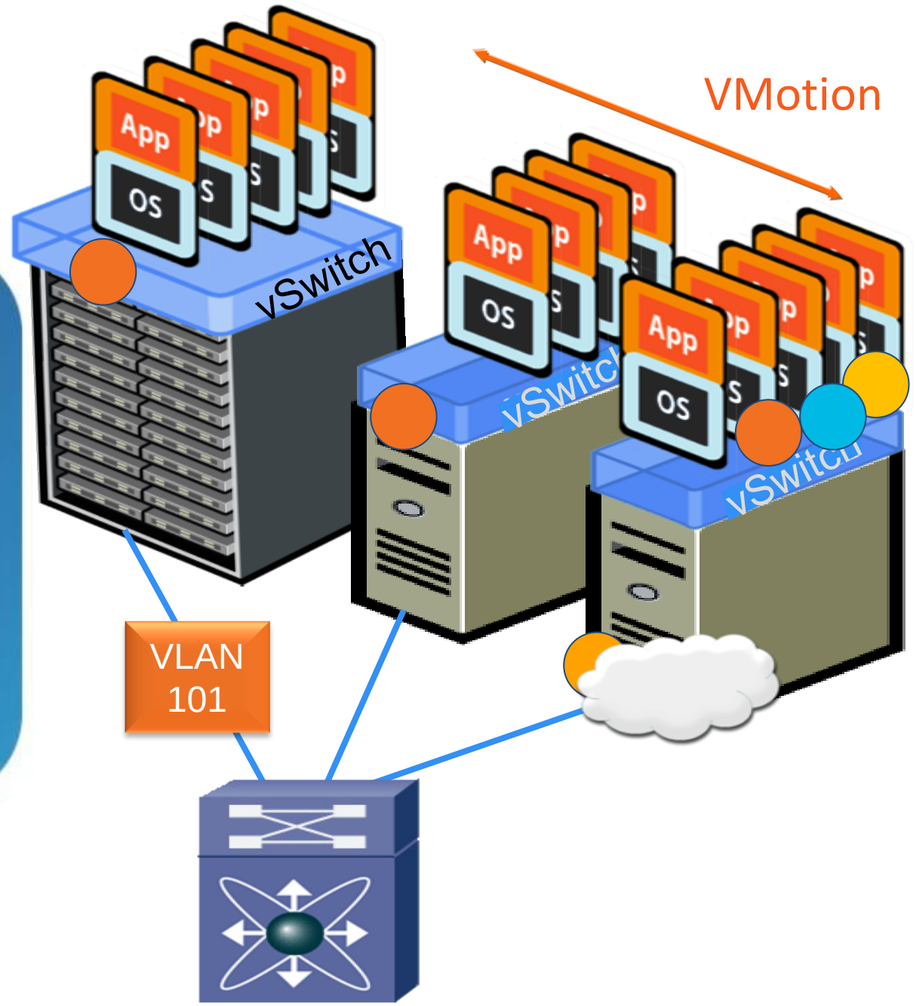


The Virtual Access



- Typically provisioned as trunk to the server running ESX
- No visibility to individual traffic from each VM
- Unable to troubleshoot, apply policy, address performance issues

VMotion and locally switched traffic



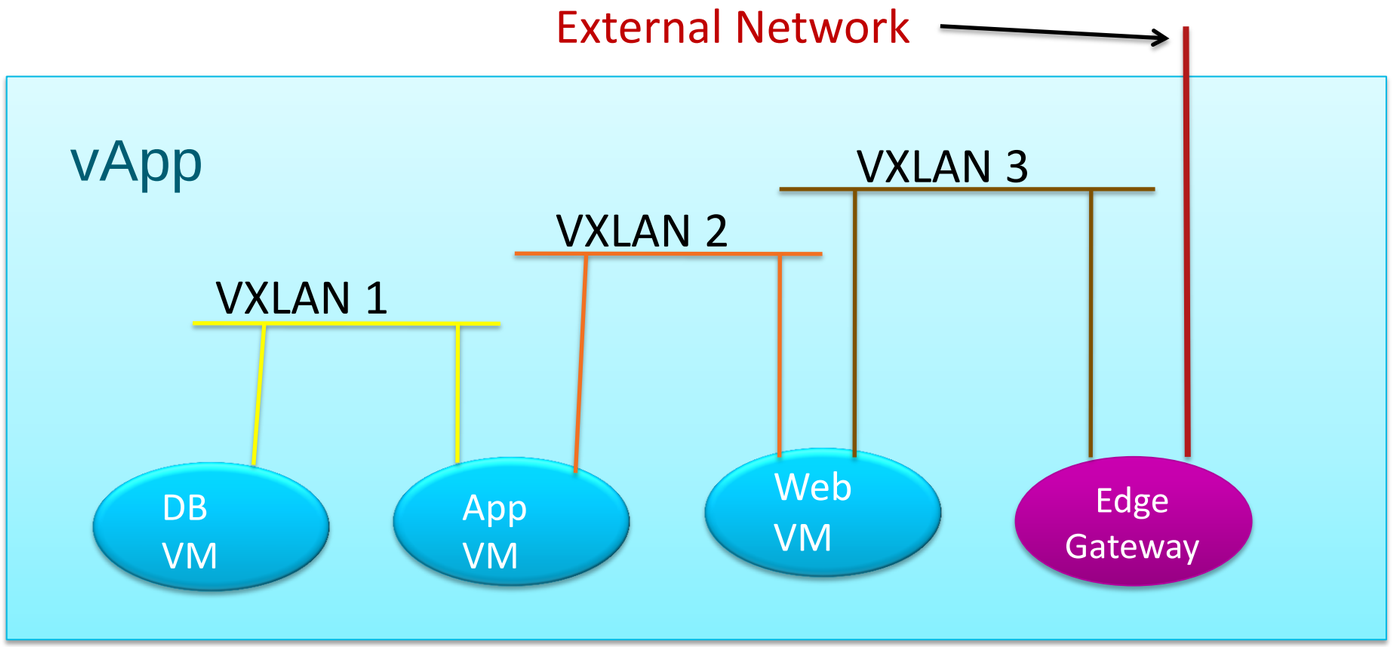
Problems:

- VMotion may move VMs across physical ports—policy must follow
- Impossible to view or apply policy to locally switched traffic
- Cannot correlate traffic on physical links—from multiple VMs
- Three solutions:
  - Virtual ports and VLAN's
  - VXLAN
  - VN-TAG and vPath

Virtual Extensible Local Area Network

(VXLAN)

- Offers virtual separation
- Currently an IETF draft submitted by Cisco, VMware, Citrix, Broadcom and others
- IP Multicast used for L2 broadcast/multicast
- Can cross Layer 3



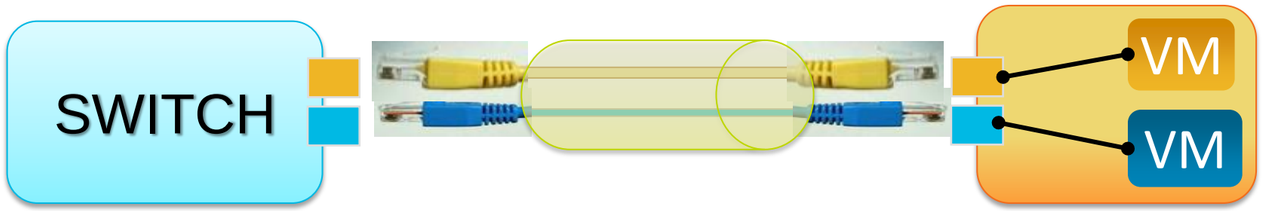
- Ethernet in IP Overlay
  - L2 frame encapsulated in UDP → 50 bytes overhead
- Uses 24bit VXLAN identified → 16M Logical networks

Outer MAC DA	Outer MAC SA	Outer 802.1Q	Outer IP DA	Outer IP SA	Outer UDP	VXLAN ID (24 bits)	Inner MAC DA	InnerMAC SA	Optional Inner 802.1Q	Original Ethernet Payload	CRC

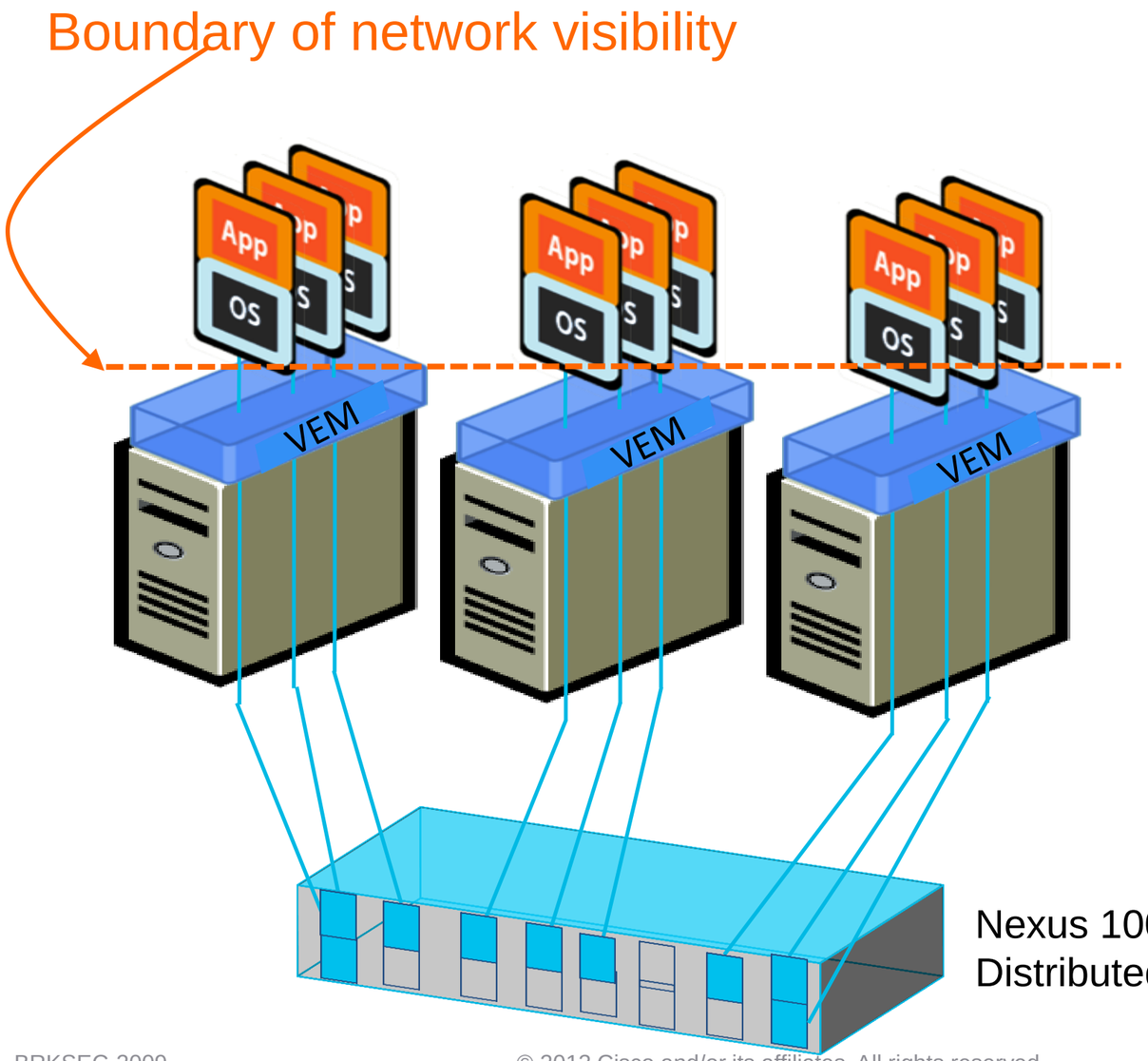
VXLAN Encapsulation → ← Original Ethernet Frame →

Virtual Network (VN)-Link

- A virtual network link between the underlying physical network and the VM
- Extends the network to the virtualisation layer by adding a special tag to the L2 frame. Carries source/destination interface ID
- Enables:
  - Policy-Based VM Connectivity
  - Mobility of Network & Security Properties
  - Non-Disruptive Operational Model
- Exists both as Software solution using Nexus 1000V or hardware solutions using the VM-FEX adapter (UCS/Nexus)



VN-Link View of the Access Layer



- Nexus 1000V and VN-Link provide visibility to the individual VMs
- Policy can now be configured per-VM and enforced on either:
  - The Nexus 1000v
  - External VN-LINK enabled devices
- Policy is now mobile within the ESX cluster

Cisco Nexus 1000V

Virtual Appliance

ASA 1000v vWAAS VSG VSM

VSM: Virtual Supervisor Module

VEM: Virtual Ethernet Module

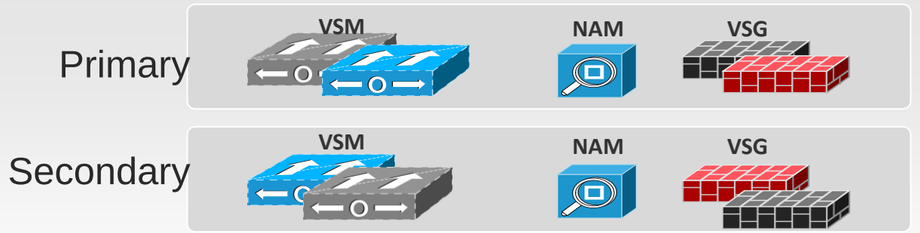
vPath: Virtual Service Data-path

VXLAN: Scalable Segmentation

VSN: Virtual Service Node

- **VSG:** Virtual Security Gateway
- **vWAAS:** Virtual WAAS
- **ASA 1000V:** Tenant-edge security

Nexus 1010 (HW Appliance)



Host multiple virtual appliances

Deploy & manage like an NX-OS switch

Access to vCenter is not required

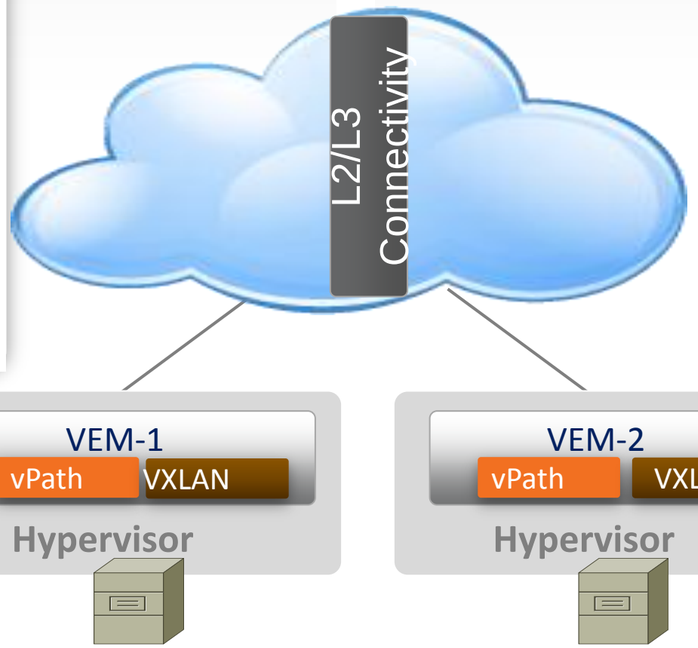
Virtual Blades

Virtual Supervisor Module (VSM)

Network Analysis Module (NAM)

Virtual Security Gateway (VSG)

Others…



vPath

- **Service Binding (Traffic Steering)**
- **Fast-Path Offload**
- **VXLAN aware**

VXLAN

- **16M LAN segments**
- **LAN segment across L3 (Mac-over-UDP encap)**
- **Submitted to IETF (with VMware, Citrix, RedHat, …)**

Nexus 1000V: Switching and Security features

Switching	▪ L2 Switching, 802.1Q Tagging, VLAN Segmentation, Rate Limiting (TX) ▪ IGMP Snooping, QoS Marking (COS & DSCP), Class-based WFQ
Security	▪ Policy Mobility, Private VLANs w/ local PVLAN Enforcement ▪ Access Control Lists (L2–4 w/ Redirect), Port Security ▪ Dynamic ARP inspection, IP Source Guard, DHCP Snooping
Provisioning	▪ Automated vSwitch Config, Port Profiles, Virtual Centre Integration ▪ Optimised NIC Teaming with Virtual Port Channel – Host Mode
Visibility	▪ VMotion Tracking, NetFlow v.9 w/ NDE, CDP v.2 ▪ VM-Level Interface Statistics ▪ SPAN & ERSPAN
Management	▪ Virtual Centre VM Provisioning, Cisco Network Provisioning, CiscoWorks ▪ Cisco CLI, Radius, TACACs, Syslog, SNMP (v.1, 2, 3) ▪ Hitless upgrade

Separation of Duties: Network and Server Teams

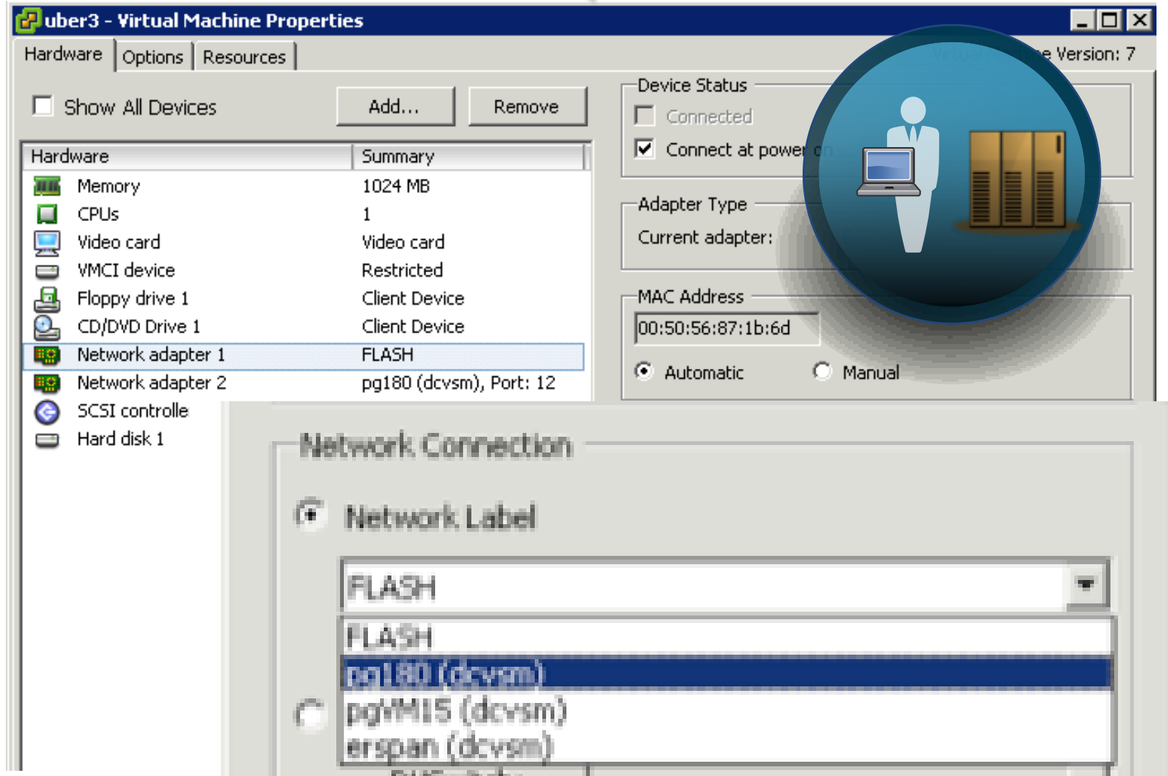
Port Profile → Port Group

vCenter API

```
port-profile vm180
  vmware port-group pg180
  switchport mode access
  switchport access vlan 180
  ip flow monitor ESE-flow input
  ip flow monitor ESE-flow output
  no shutdown
  state enabled

interface Vethernet9
  inherit port-profile vm180

interface Vethernet10
  inherit port-profile vm180
```



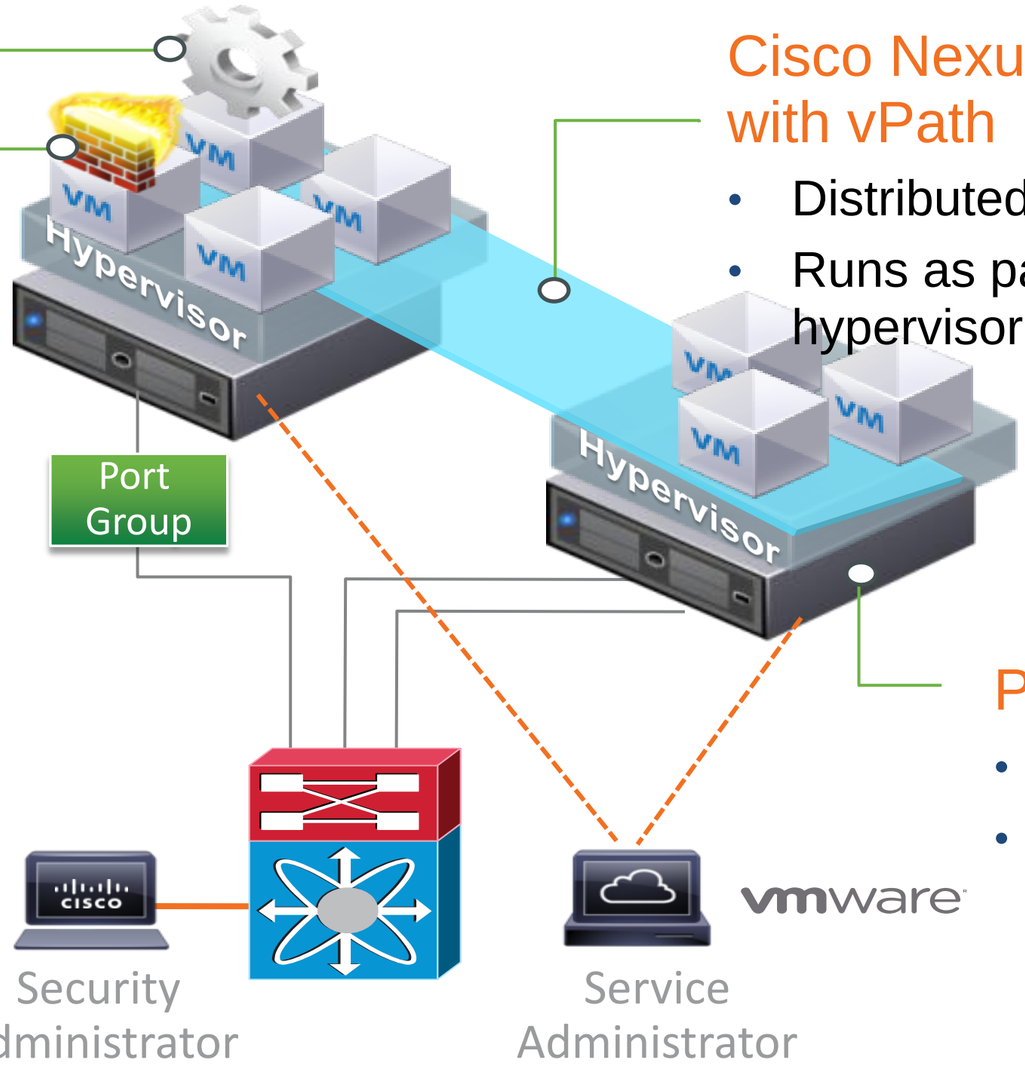
Cisco Virtual Security Gateway (VSG)

Virtual Network Management Center

- Management console for VSG
- Runs on one of the VMs

Virtual Security Gateway

- Software-based firewall
- Runs on one of the VMs
- Provides zone-based policy and secure segmentation for all VMs



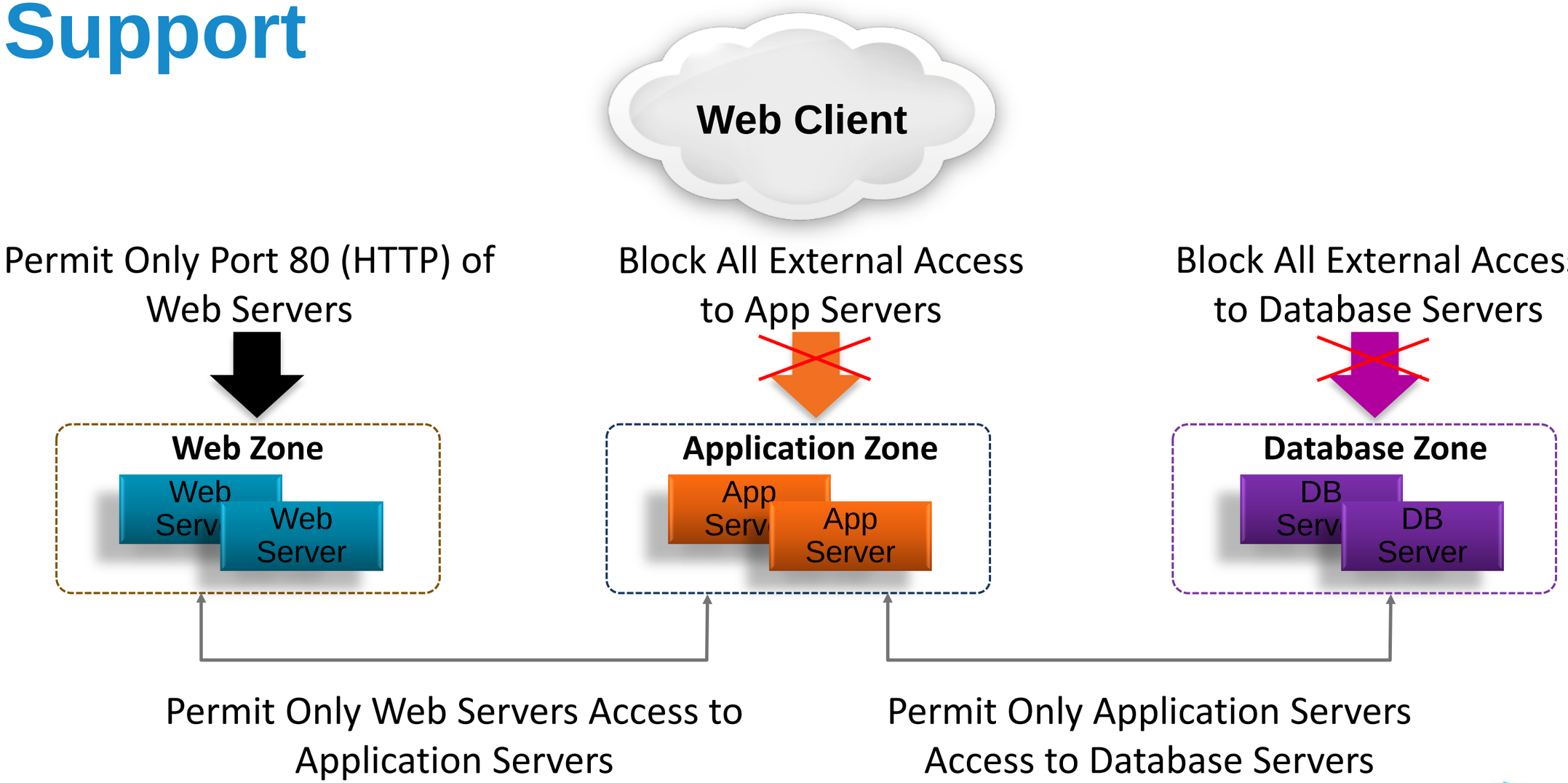
Cisco Nexus® 1000V with vPath

- Distributed virtual switch
- Runs as part of hypervisor

Physical Host

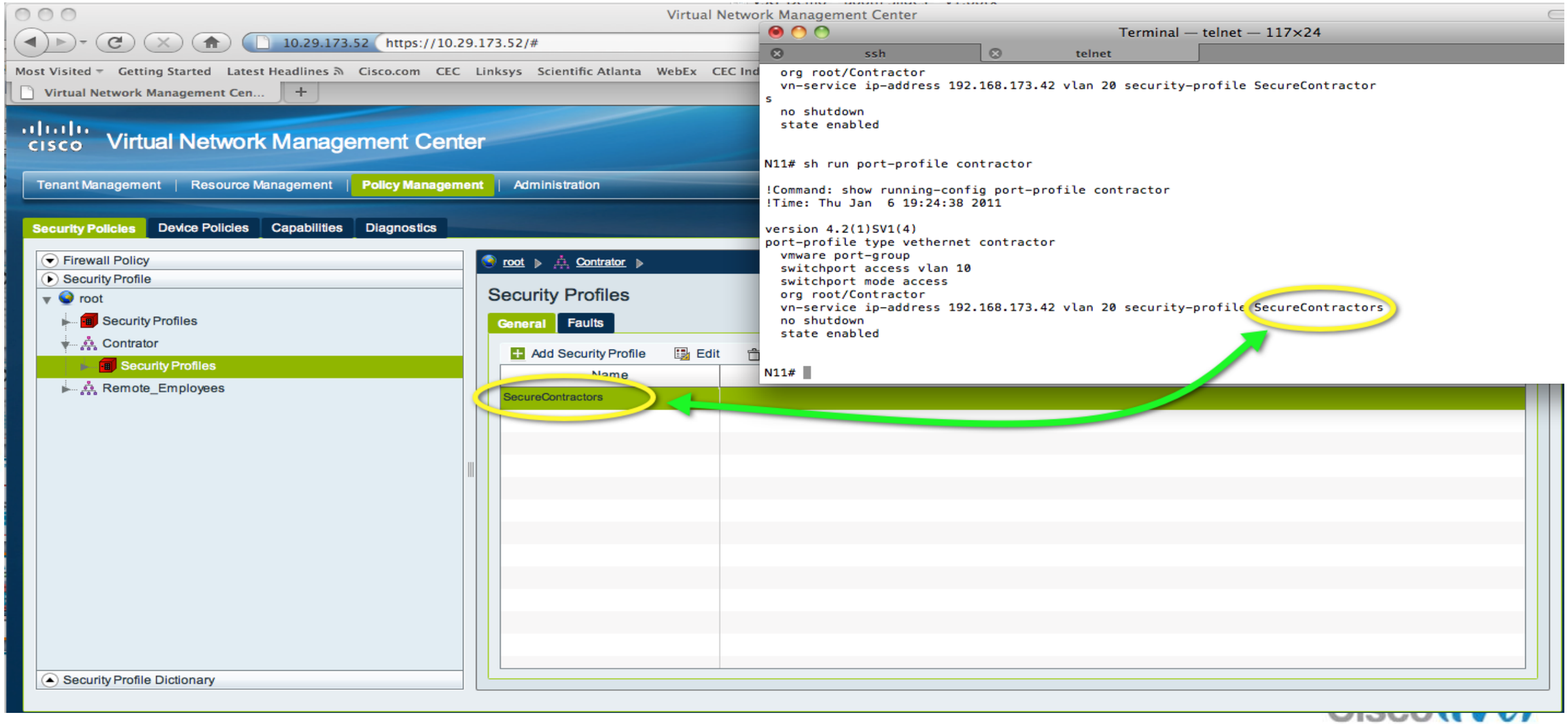
- Cisco UCS™
- Other x86 server

VSG: Zone-Based Policy and VM Mobility Support



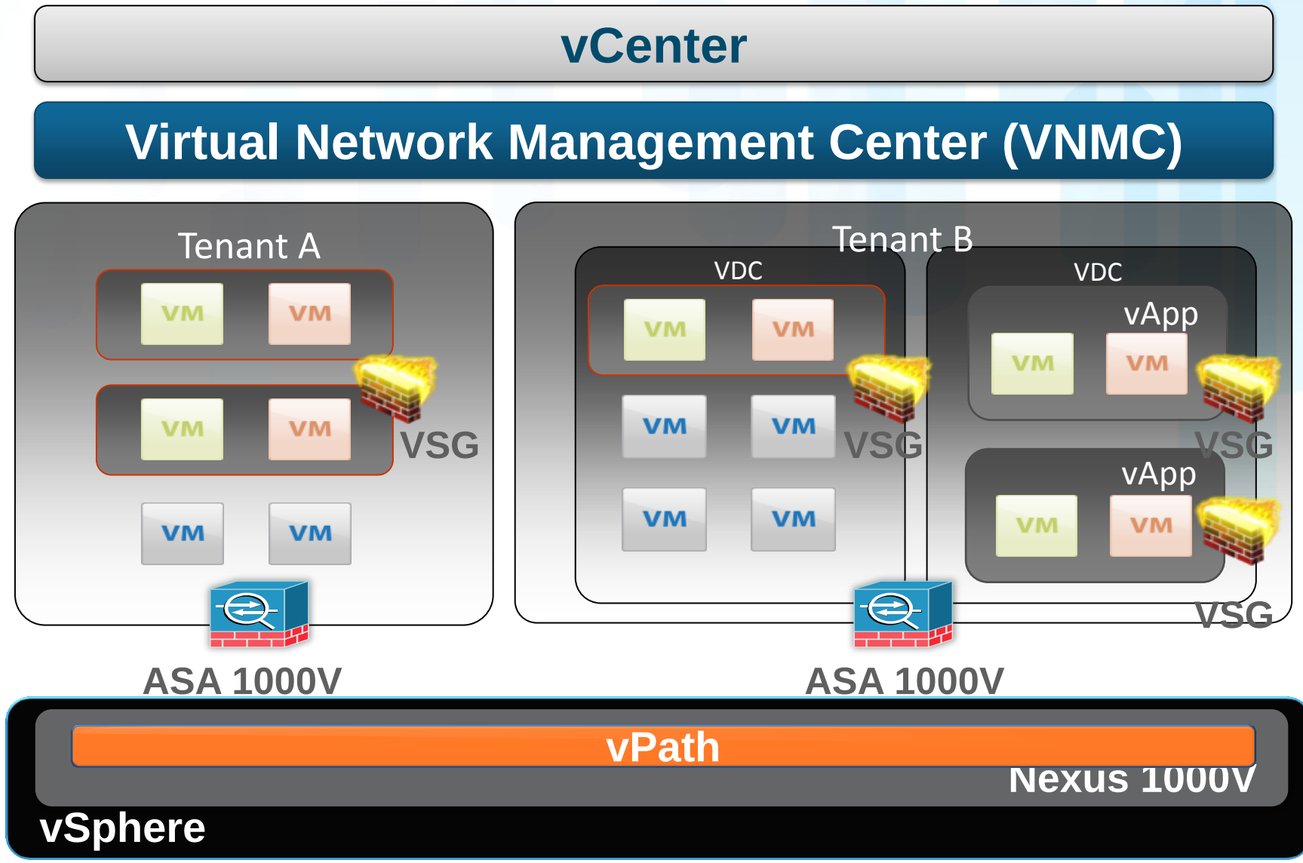
Separation of Duties: Network and Security Teams

VSG: Security Profile to Port Profile



ASA1000v with vPath Support

- Proven Cisco Security…Virtualised
- Collaborative Security Model
  - VSG for intra-tenant secure zones
  - ASA 1000V for tenant edge controls
- Seamless Integration
  - With Nexus 1000V & vPath
- Scales with Cloud Demand
  - Multi-instance deployment for horizontal scale-out deployment

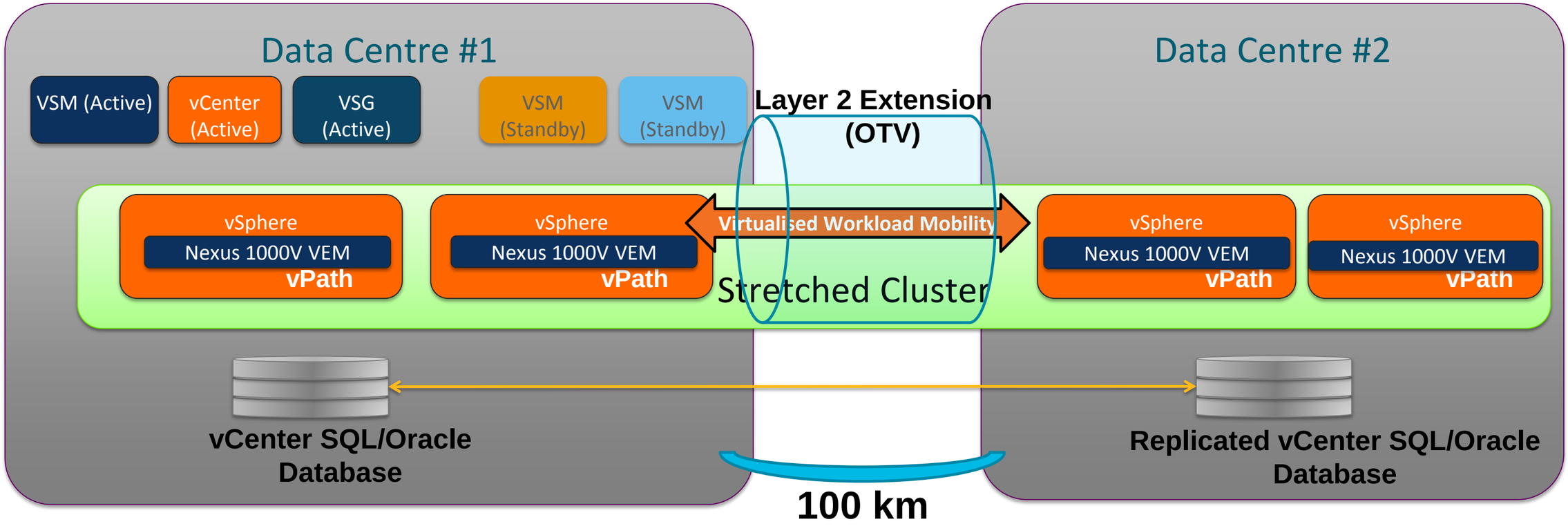


vPath— The Intelligent Virtual Network

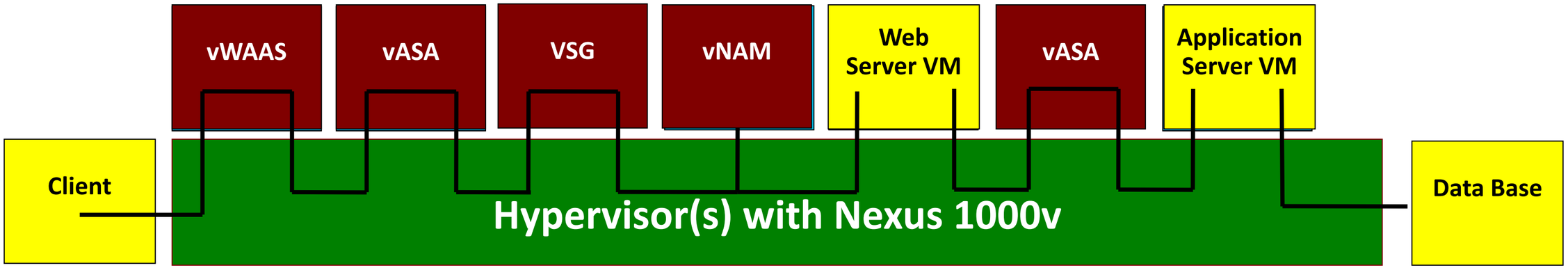
- vPath is intelligence build into Virtual Ethernet Module (VEM) of Nexus 1000V (1.4 and above)
- vPath has two main functions:
  - Intelligent Traffic Steering
  - Offload processing via Fastpath from virtual Service Nodes to VEM
- Dynamic Security Policy Provisioning (via security profile)
- vPath is Multi-tenant Aware
- Leveraging vPath enhances the service performance by moving the processing to Hypervisor

vPath Across Multiple Datacentres

Nexus 1000V VSM Pair & VSG Pair
(or VSG/VSG hosted on Nexus 1010s)



Integrating Virtual Service Nodes – vPath 2.0



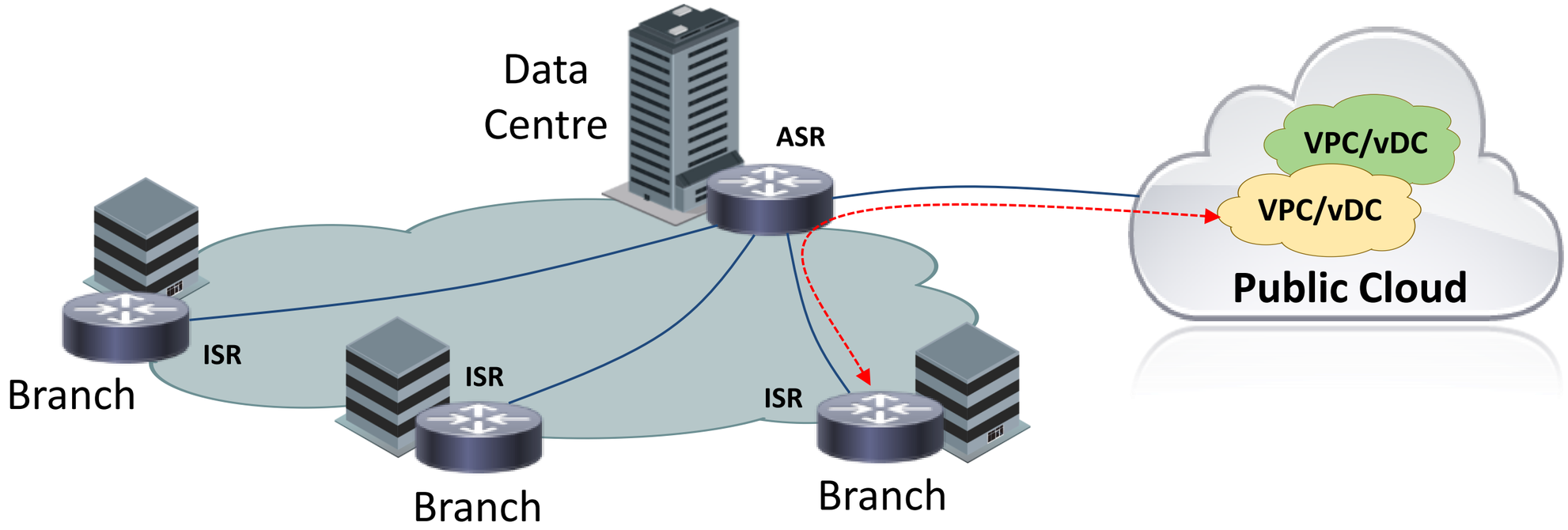
- A Data packet enters vPath and is sent to the first VSN according to a pre-defined policy
- A VSN can either pass it back to vPath where it follows the original policy or it can redirect the data packet to a different VSN
- vPath supports
  - Fastpath
  - Chaining multiple services
  - Stateful return path
  - Clustering for scale

Securing Cloud Infrastructure

Extending the Private Cloud into Virtual Private Clouds – CSR 1000V

External Cloud Networking Challenges

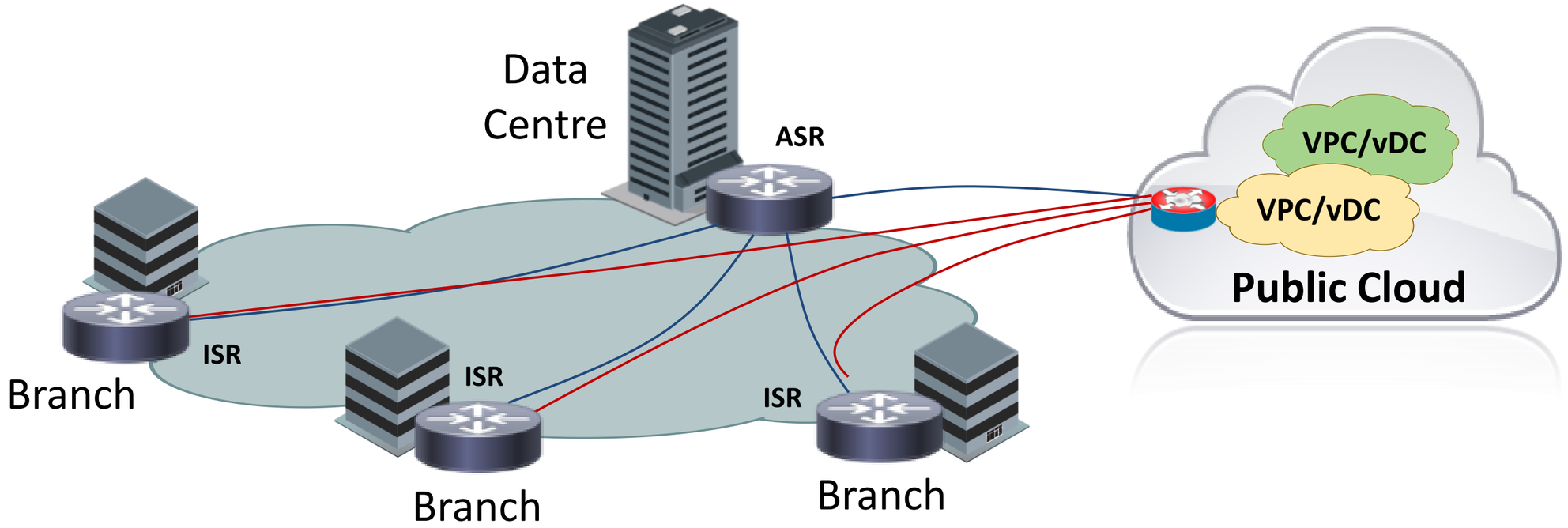
Extending Enterprise WAN to External Clouds



- Challenges
  - Inconsistent VPN Configuration
  - Incompatible IP addressing
  - Incomplete network services
  - Different management tools
  - No WAN optimisation options
  - Inability to prioritise traffic

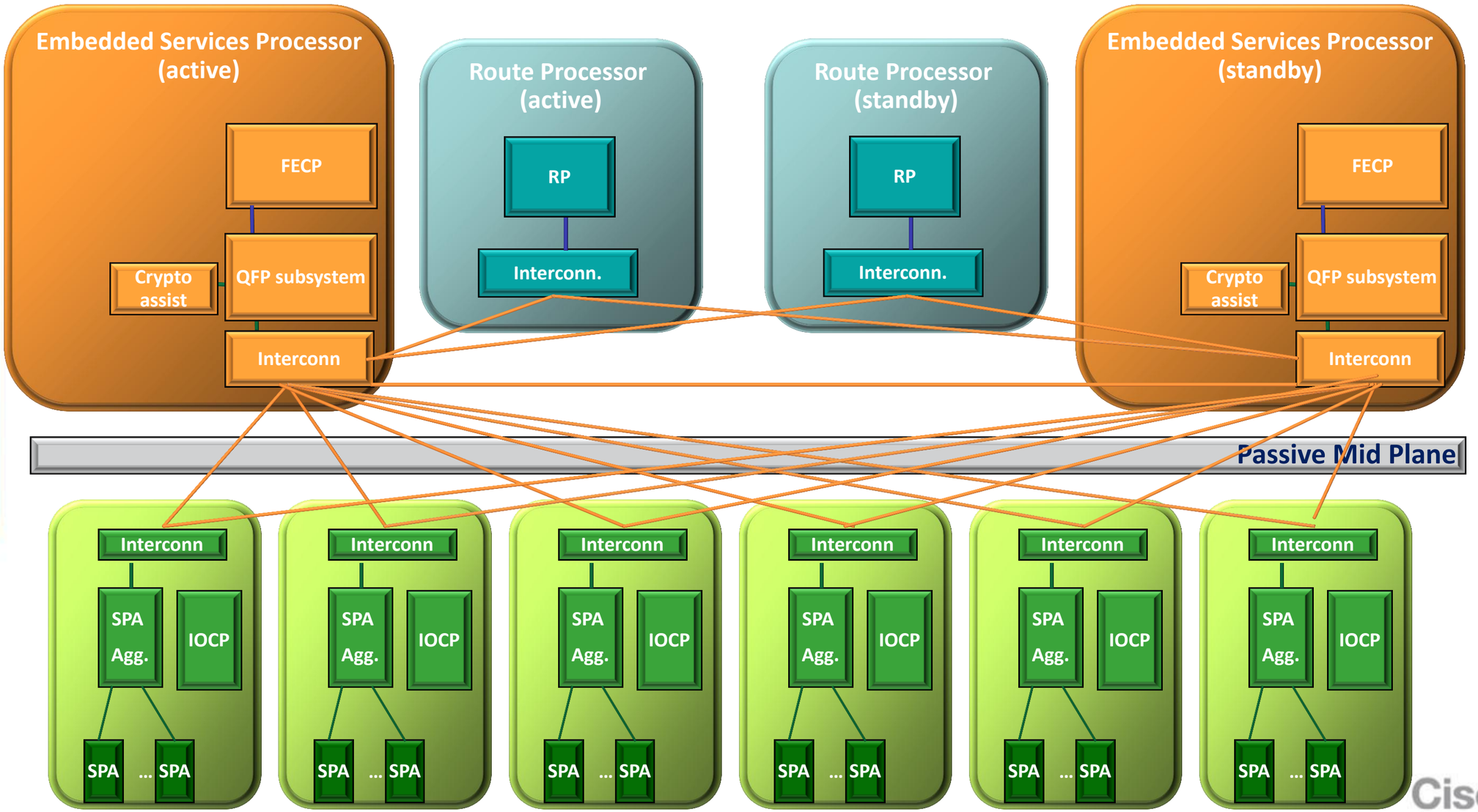
Cisco Cloud Services Router (CSR 1000v)

Cisco Cloud Services Router (CSR 1000v)

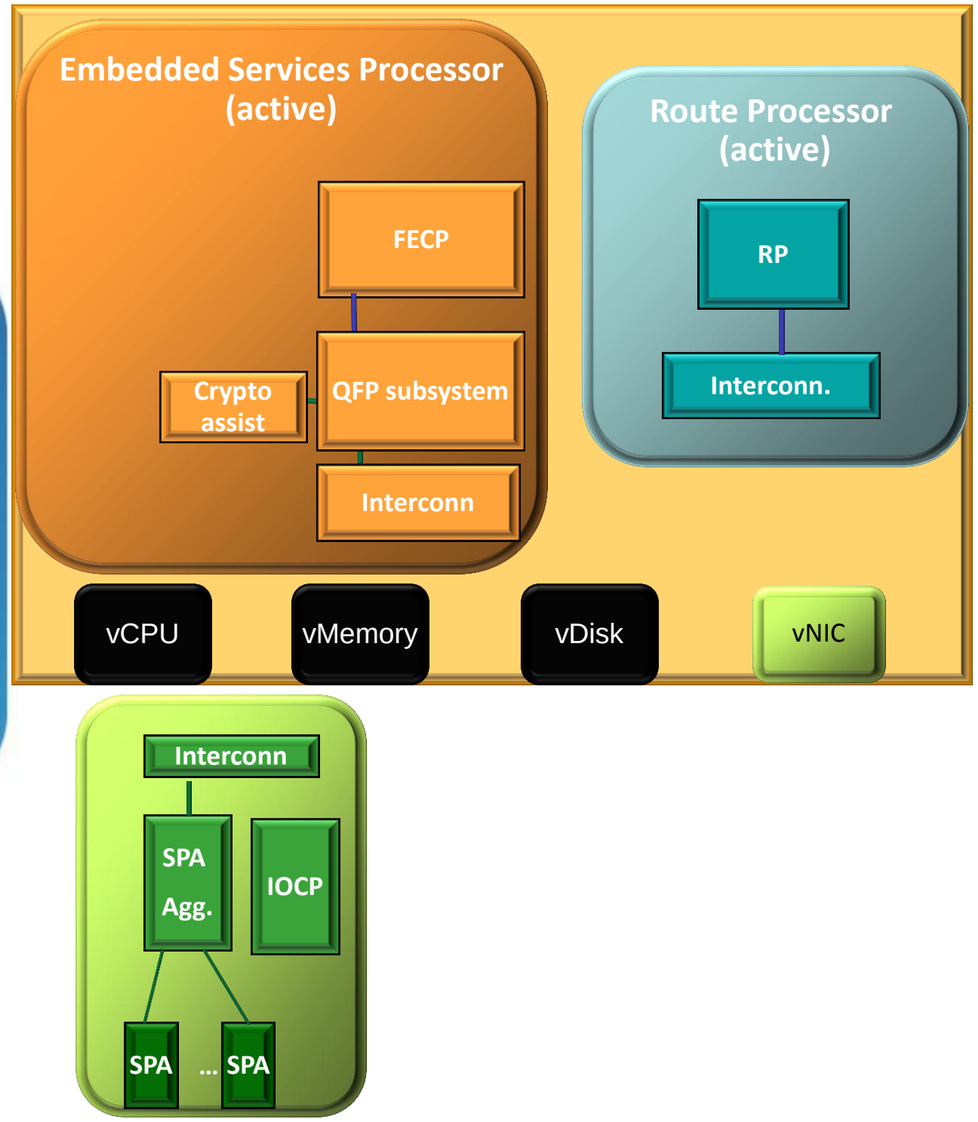


- Solutions
  - Consistent VPN Configuration
  - Compatible IP addressing
  - Complete network services
  - Consistent management tools
  - Intercept and RedirectWAN optimisation options
  - Classification and prioritisation

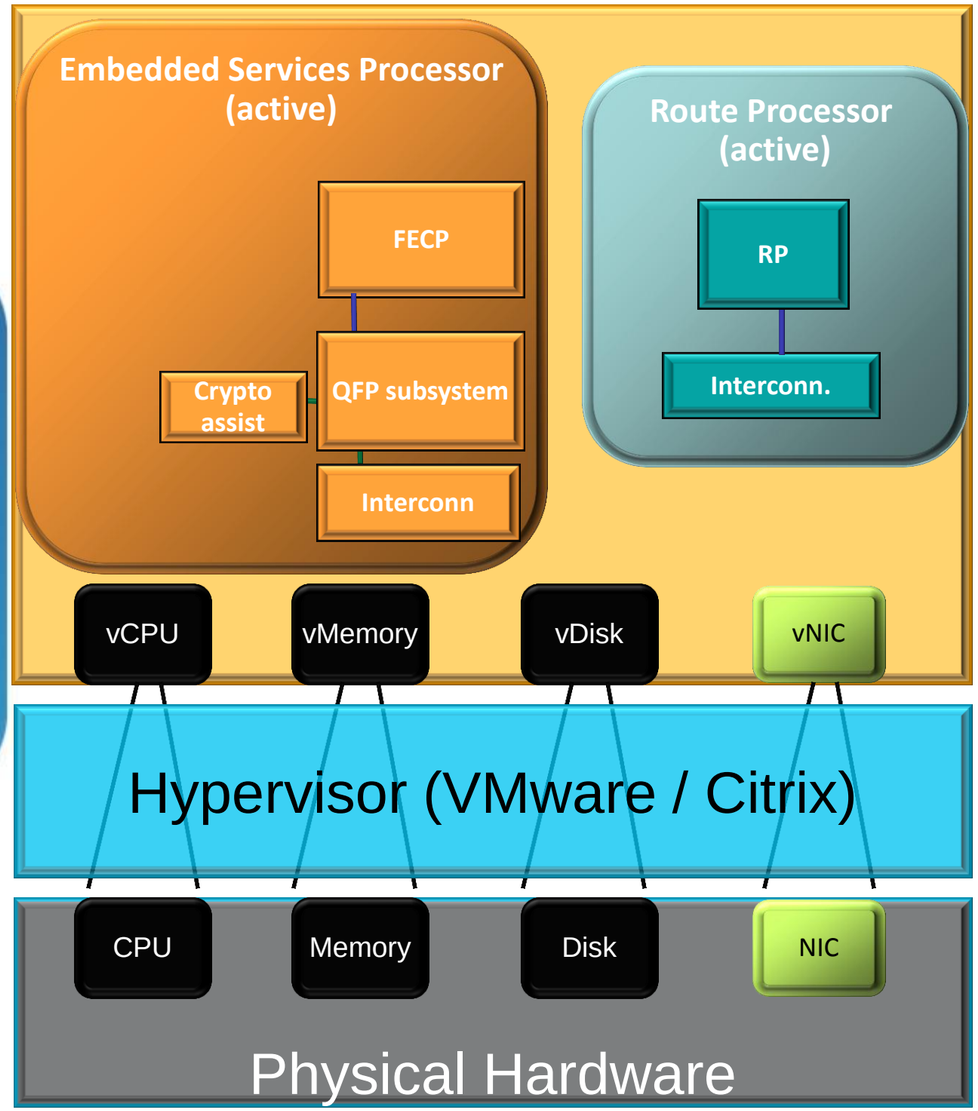
Architecture (IOS XE)



Architecture (IOS XE CE – Cloud Edition)



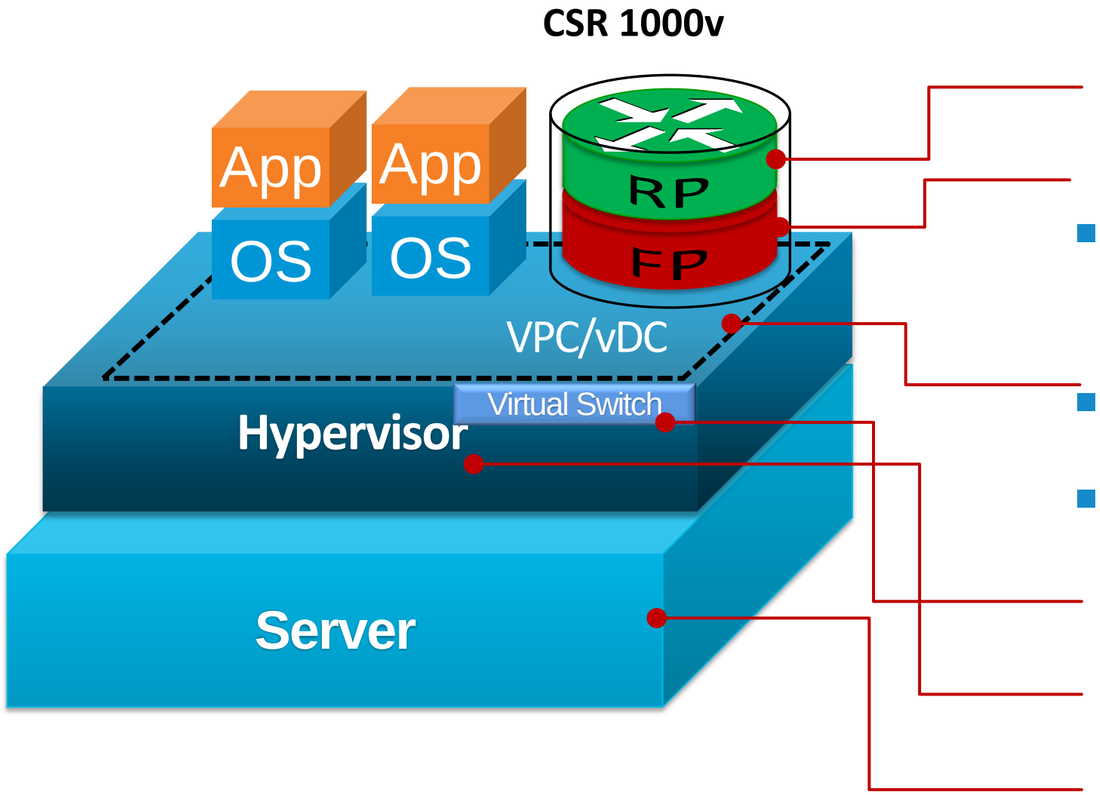
Architecture (IOS XE CE – Cloud Edition)



- Cisco IOS XE Cloud Edition
  - Selected feature set of Cisco IOS XE
  - Virtual Route Processor (RP)
  - Virtual Forwarding Processor (FP)
- Virtual Private Cloud/Data Centre Gateway
- Optimised for single tenant use cases
- Agnostic to Other Infrastructure Elements
  - Hypervisor agnostic
  - Virtual switch agnostic
  - Server agnostic

CSR 1000v

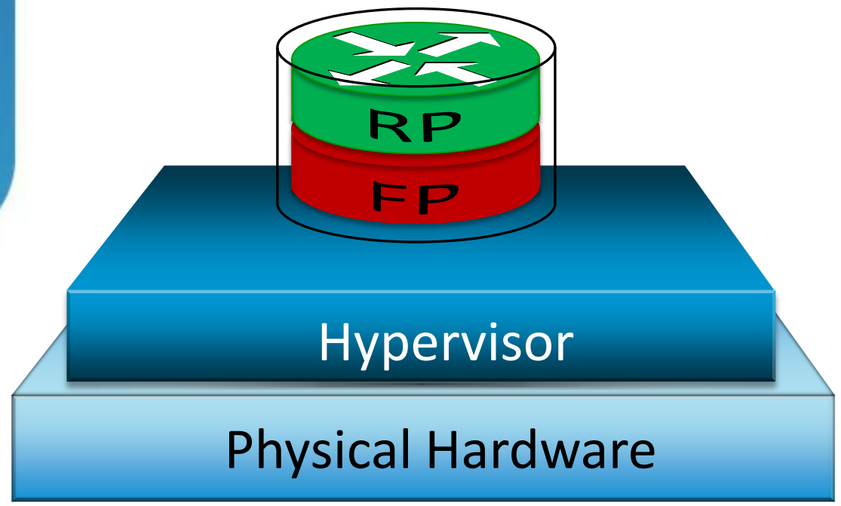
Cisco IOS XE Software in Virtual Form-factor

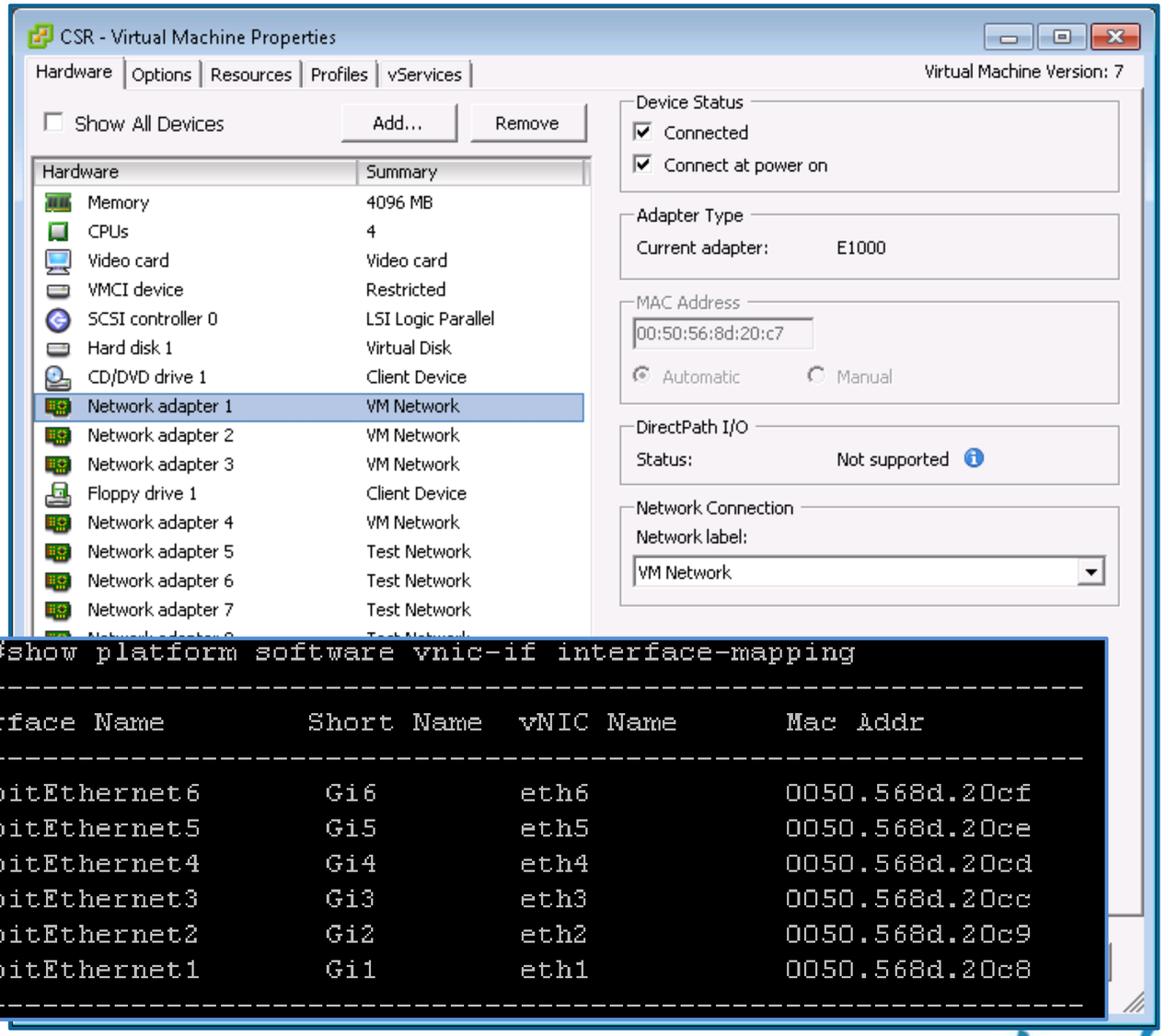


- Cisco IOS XE Cloud Edition
  - Selected feature set of Cisco IOS XE
  - Virtual Route Processor (RP)
  - Virtual Forwarding Processor (FP)
- Virtual Private Cloud/Data Centre Gateway
- Optimised for single tenant use cases
- Agnostic to Other Infrastructure Elements
  - Hypervisor agnostic
  - Virtual switch agnostic
  - Server agnostic

Virtual Network Interfaces

- Max vNICs per Hypervisor
- E1000, VMXNET2, VMXNET3
- Sub-interface Available

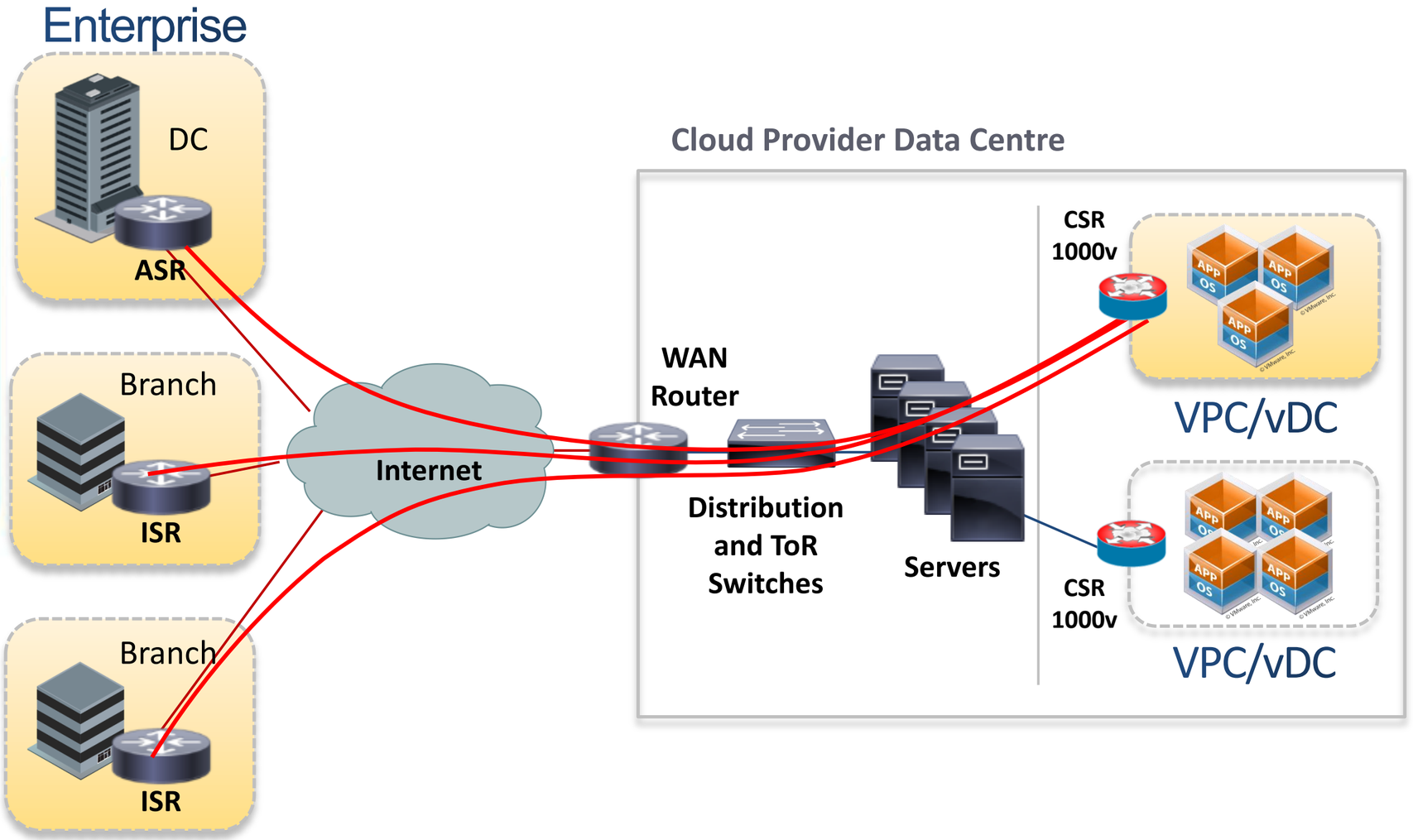





```
CSR_1#show platform software vnic-if interface-mapping
------------------------------------------------------------------
 Interface Name         Short Name  vNIC Name       Mac Addr
------------------------------------------------------------------
 GigabitEthernet6        Gi6         eth6            0050.568d.20cf
 GigabitEthernet5        Gi5         eth5            0050.568d.20ce
 GigabitEthernet4        Gi4         eth4            0050.568d.20cd
 GigabitEthernet3        Gi3         eth3            0050.568d.20cc
 GigabitEthernet2        Gi2         eth2            0050.568d.20c9
 GigabitEthernet1        Gi1         eth1            0050.568d.20c8
------------------------------------------------------------------
```

Use Case: Secure VPN Gateway

Scalable, Dynamic, and Consistent Connectivity to External Cloud



Challenges

- Inconsistent security
- High network latency
- Limited scalability

Solutions

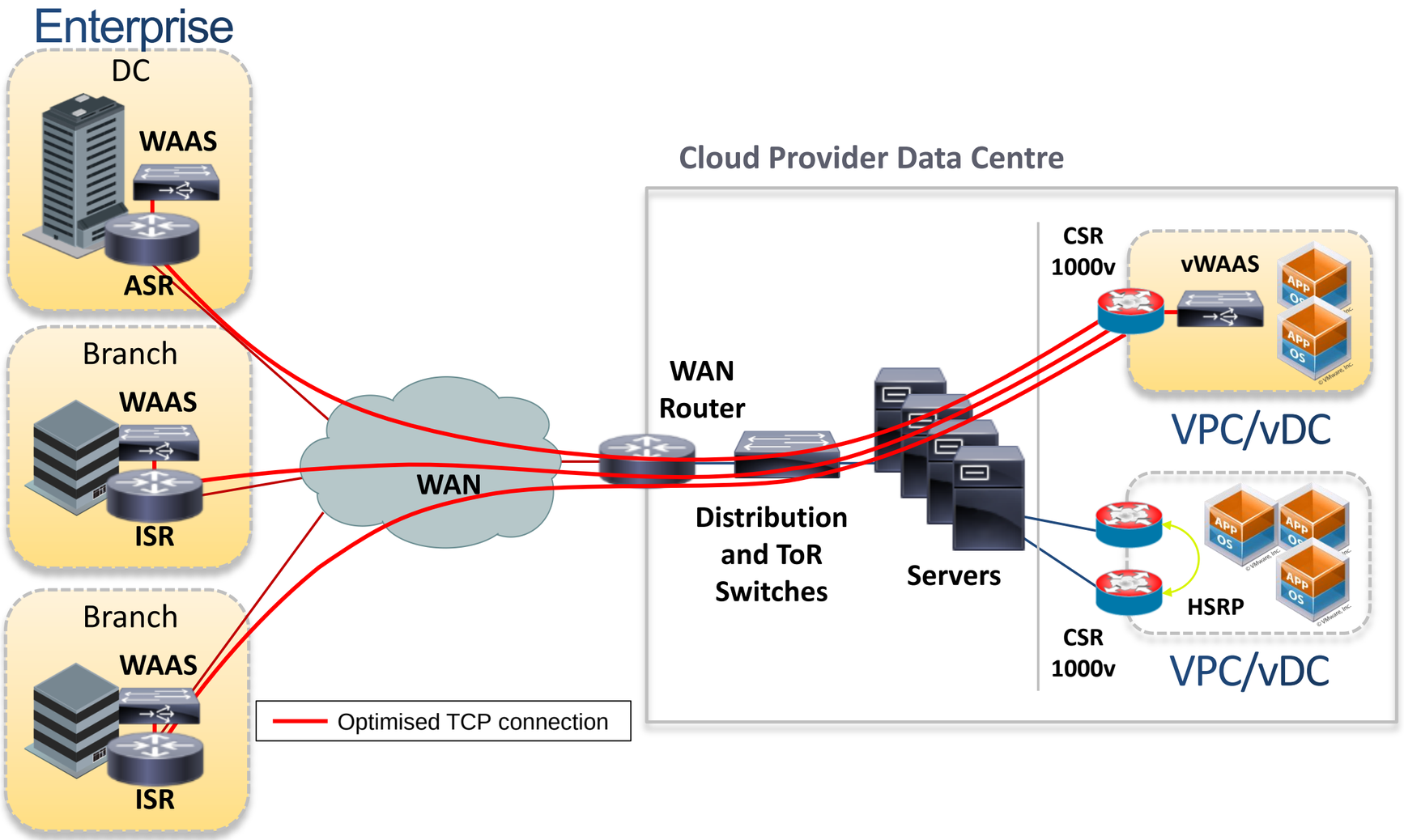
- IPSec VPN, DMVPN, EZVPN, FlexVPN
- Routing and addressing
- Firewall, ACLs, AAA

Benefits

- Direct, secure access
- Scalable, reliable VPN
- Operational simplicity

Use Case: Traffic Control and Management

Comprehensive Networking Services Gateway in External Cloud



Challenges

- Response time of apps
- Application prioritisation
- Connectivity resiliency

Solutions

- AppNav for WAAS
- QoS prioritisation
- HSRP VPN resiliency

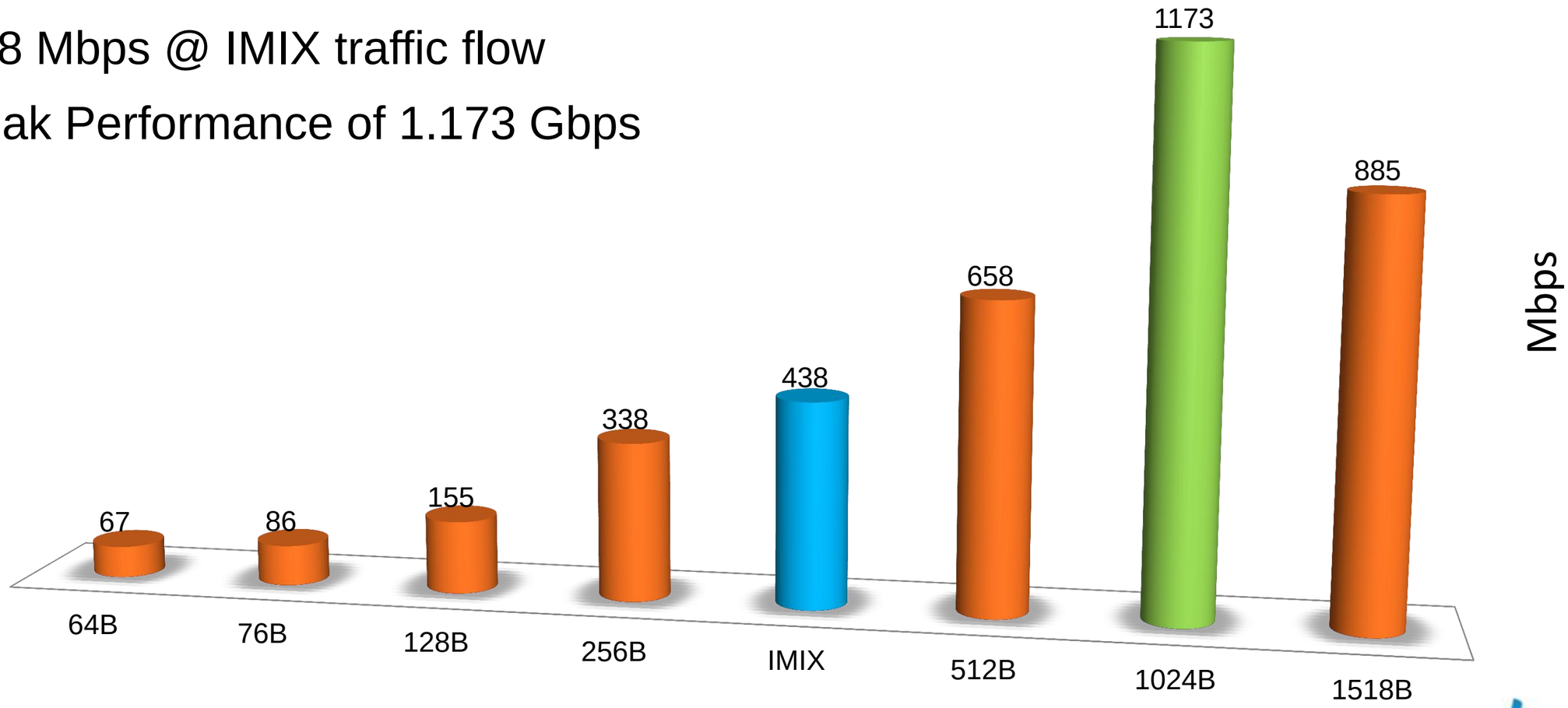
Benefits

- Rich portfolio of network features and services
- Single point of control

Performance

CEF

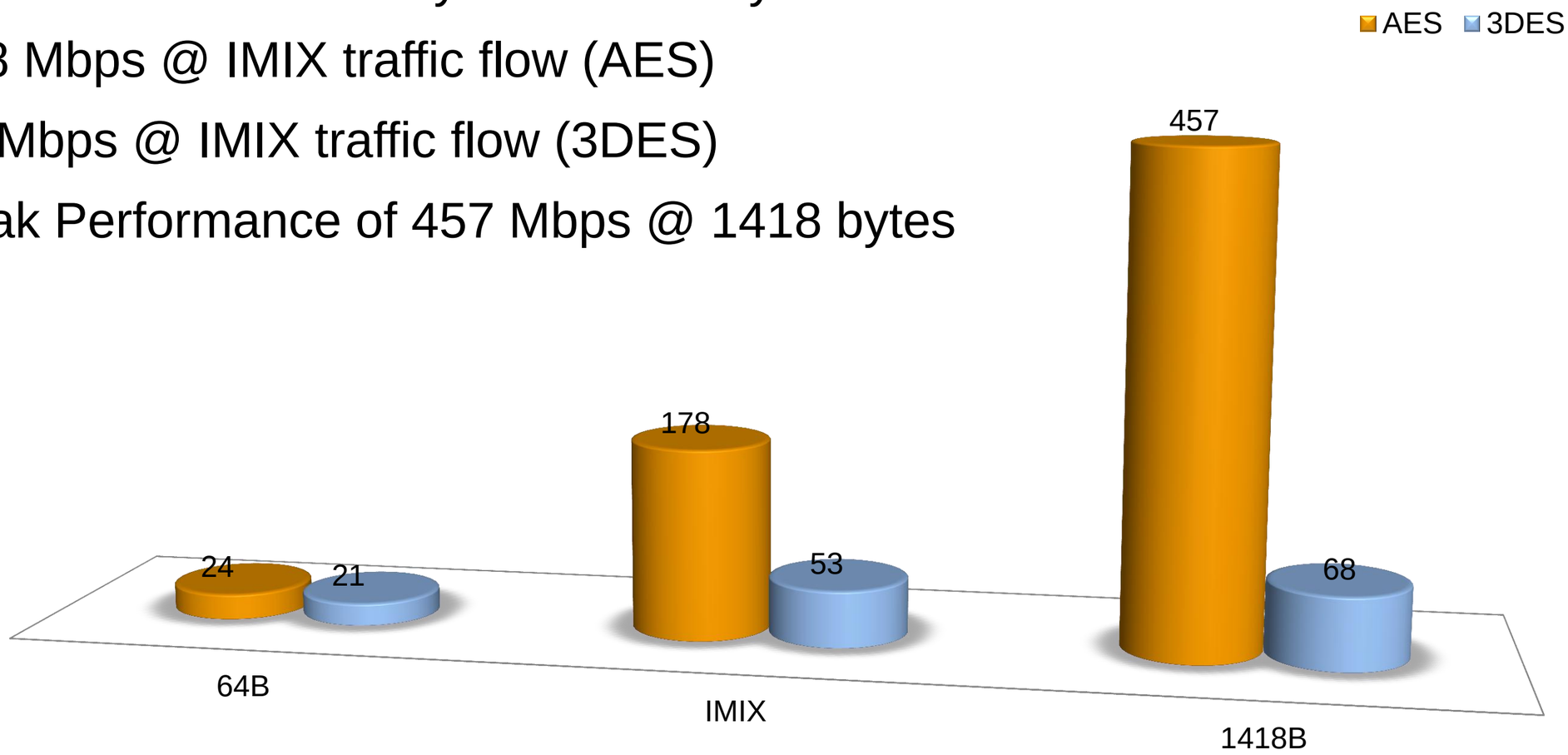
- Packet sizes from 64 bytes to 1518 bytes
- 438 Mbps @ IMIX traffic flow
- Peak Performance of 1.173 Gbps



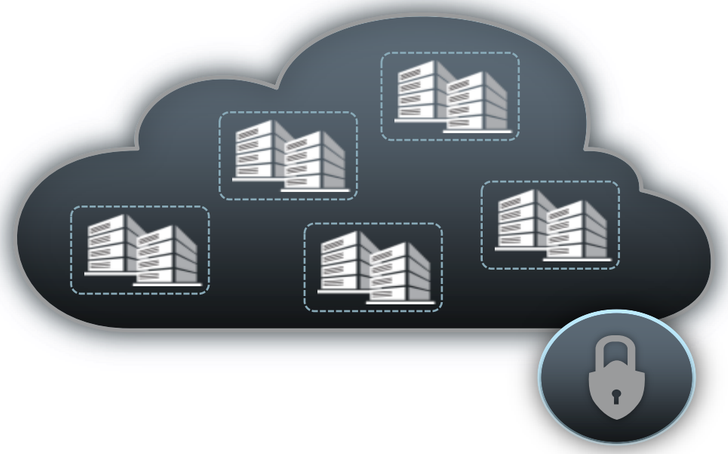
Performance

IPSec

- Packet sizes from 64 bytes to 1418 bytes
- 178 Mbps @ IMIX traffic flow (AES)
- 53 Mbps @ IMIX traffic flow (3DES)
- Peak Performance of 457 Mbps @ 1418 bytes

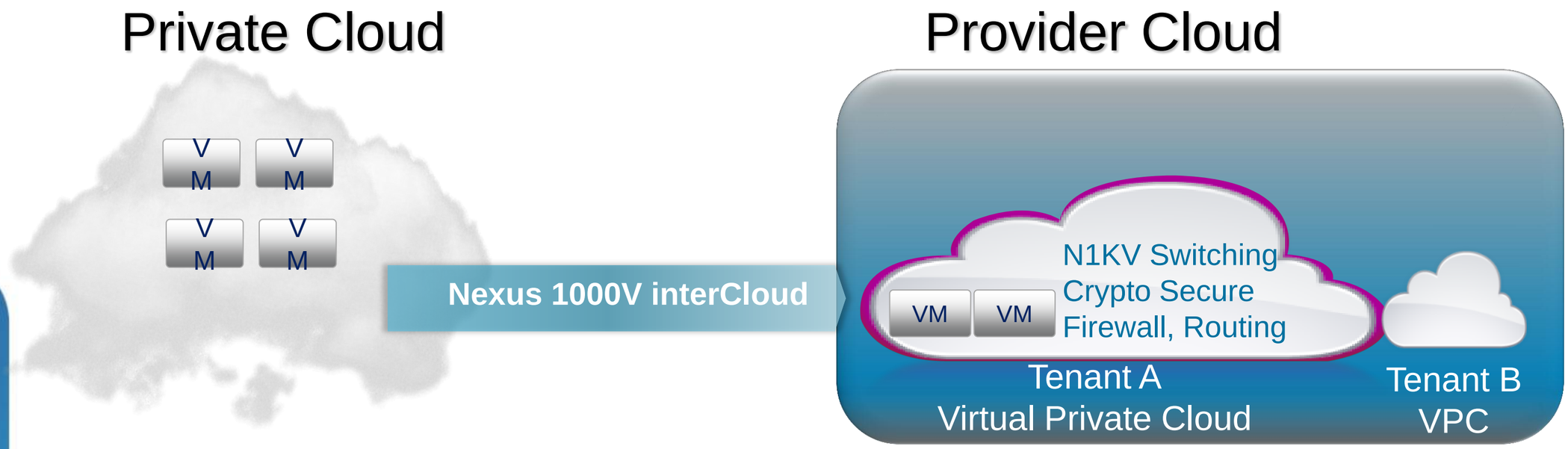


Securing Cloud Infrastructure Nexus 1000v interCloud



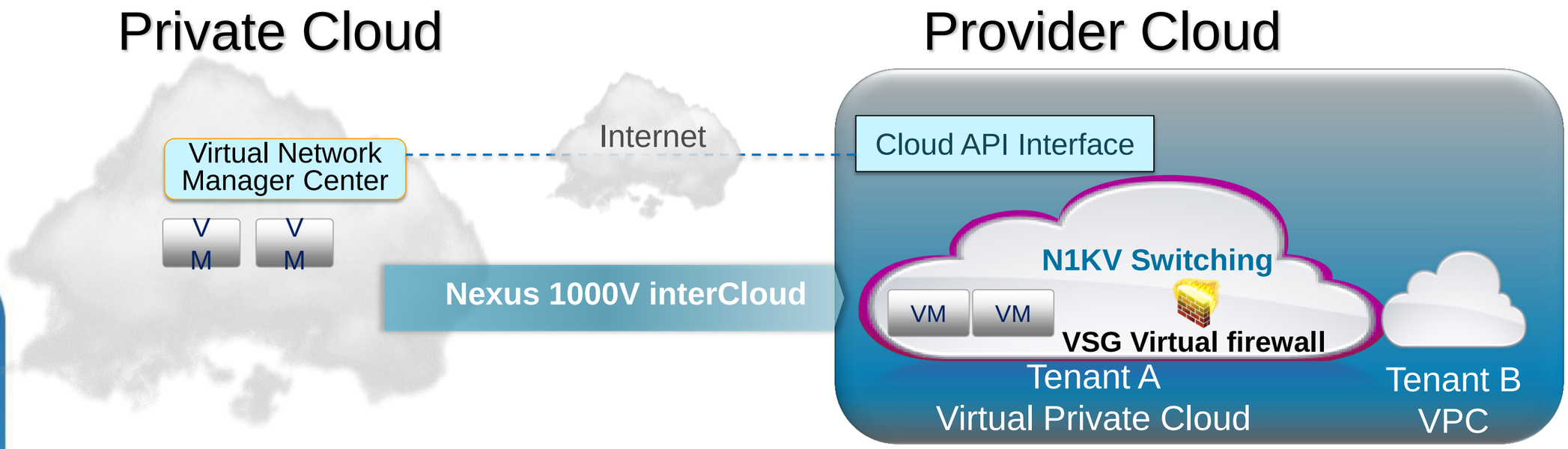
New!

Nexus1000V interCloud



Security	Secure connectivity, End to end encryption
Simplicity	Single pane of management, Consistent policies
Services	Advanced network services, rich NX-OS features
Flexibility	Multi cloud, Multi hypervisor, Multi Service

Nexus1000V interCloud

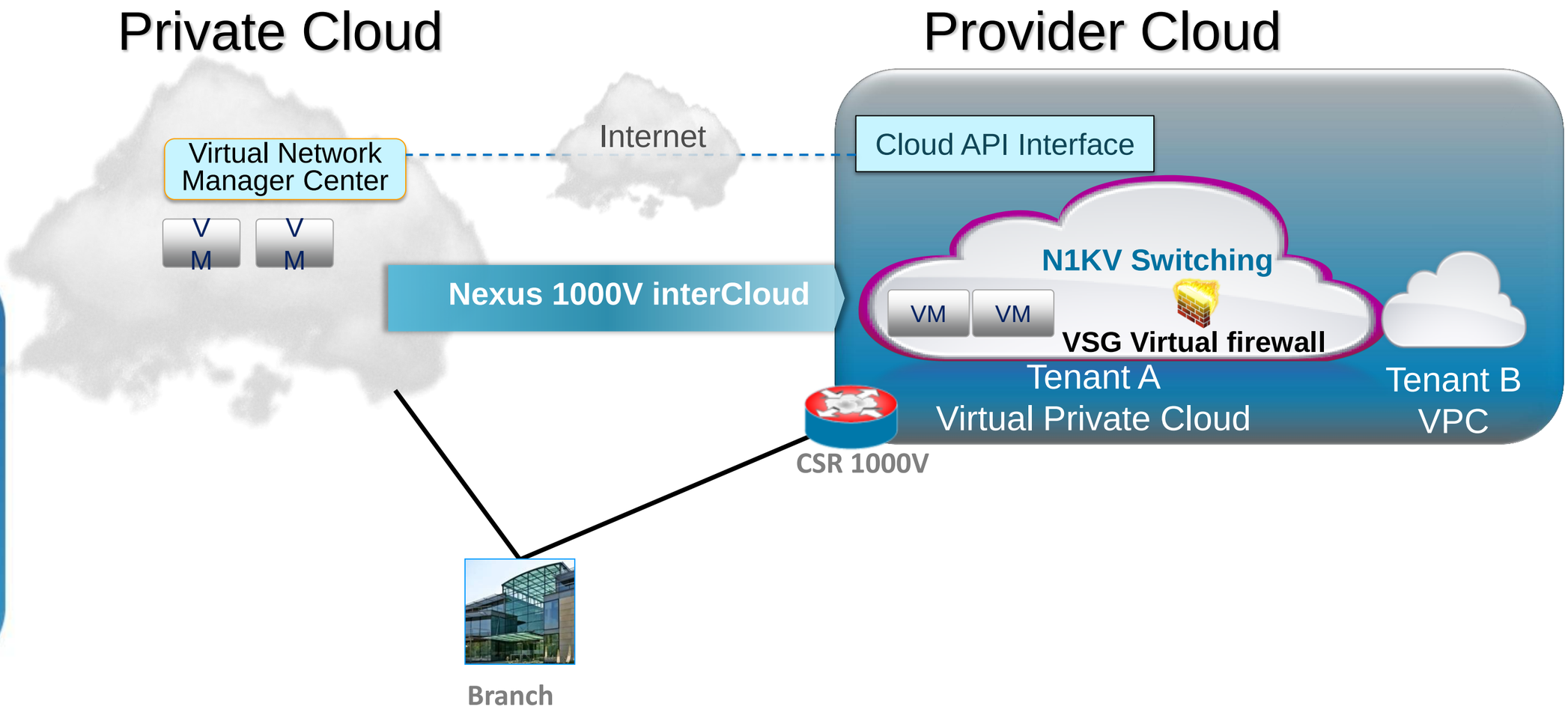


Virtual Switch for Cloud

Single pane of management

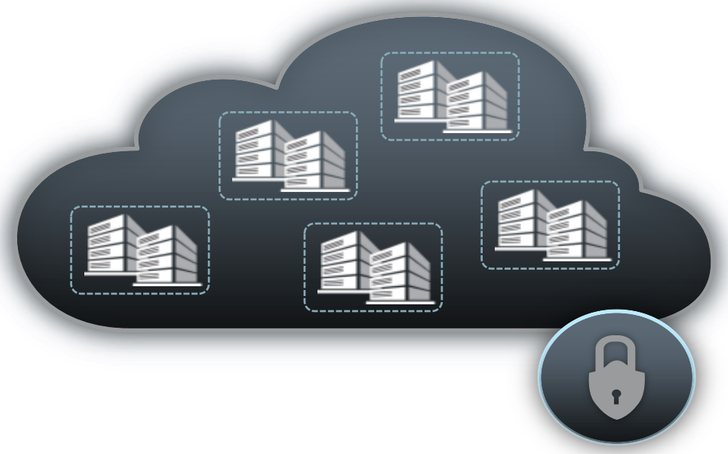
Cloud Network Services

Nexus1000V interCloud



CSR 1000V integration makes it possible to access the VPC directly across the Internet in a scalable, secure way

Securing Cloud Infrastructure

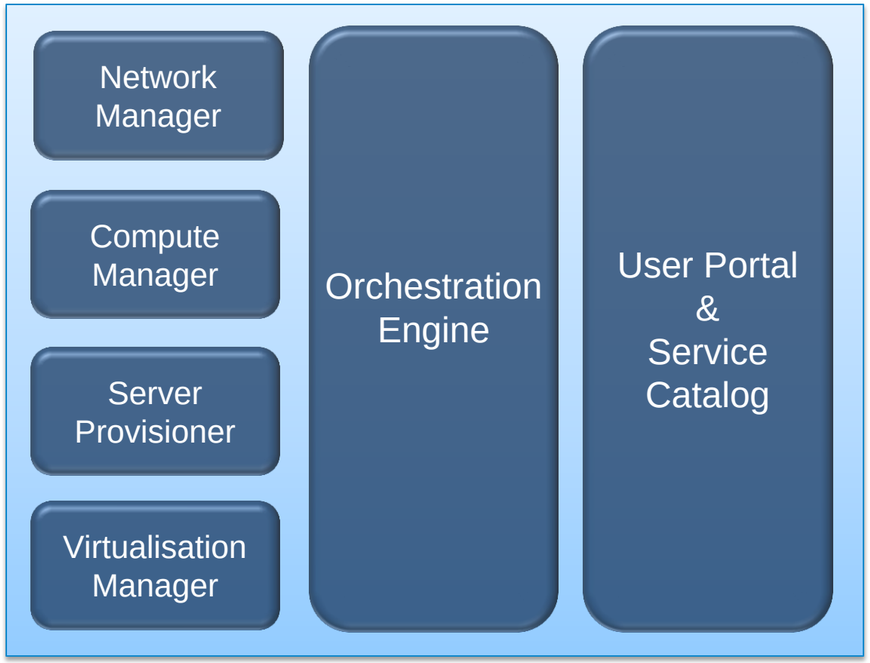


Management and Orchestration

Cisco Intelligent Automation for Cloud – Cisco IAC

Orchestration and Management Software

- Service catalog and self-service portal – Cisco Cloud Portal
- Global orchestration and reporting – Cisco Process Orchestrator
- Bare metal provisioning – Cisco Server Provisioner
- Multi-tenant network provisioning – Cisco Network Services Manager
- Adapter framework to communicate to compute, virtualisation and storage domain managers



Cisco IAC Components Explained

Compute Manager

UCS Manager

Network Manager

LINESIDER TECHNOLOGIES

Orchestration Engine

TIDAL SOFTWARE

User Portal & Service Catalog

newScale®

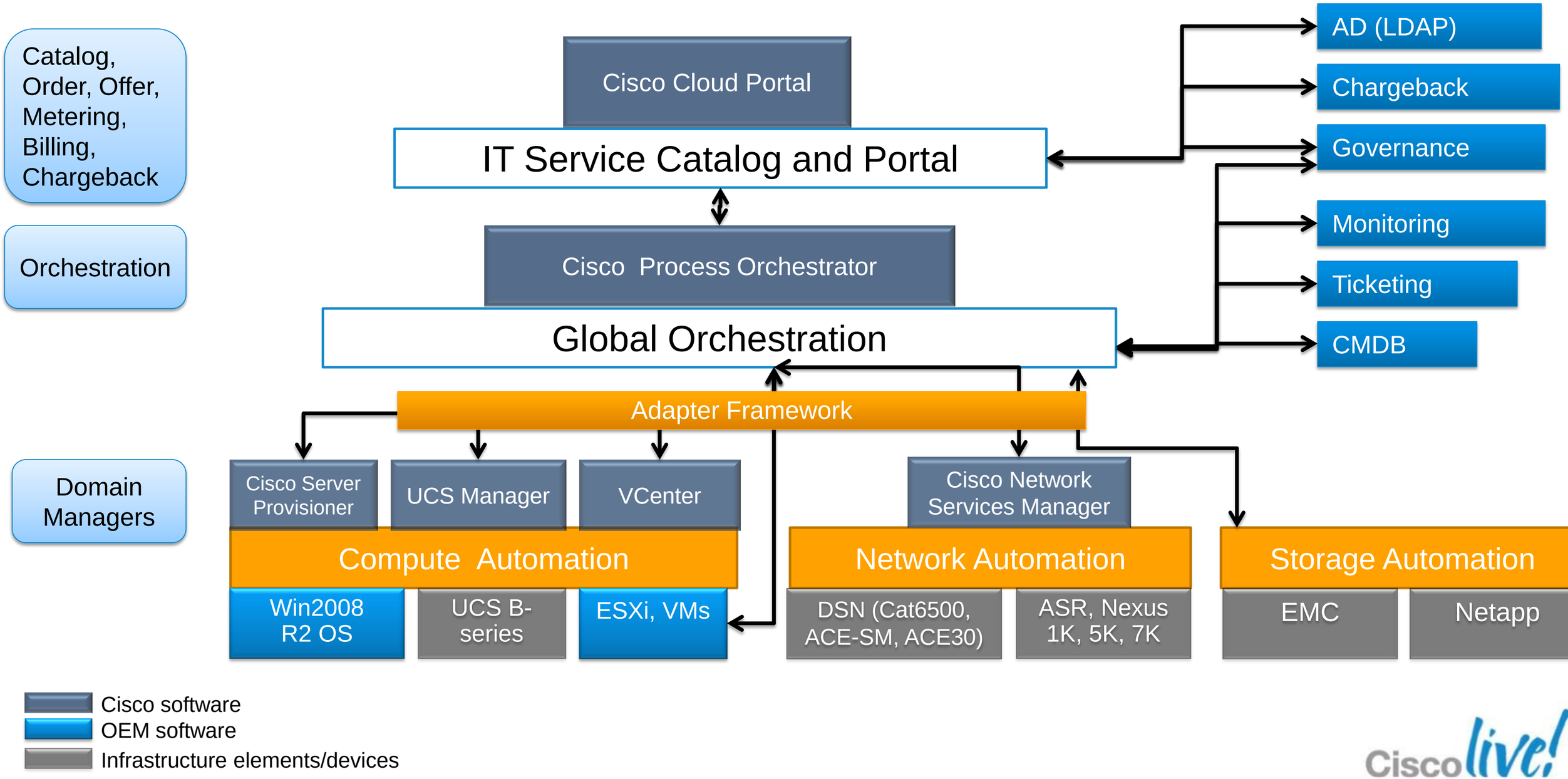
Virtualisation Manager

vCenter

Server Provisioner

Cisco Server Provisioner

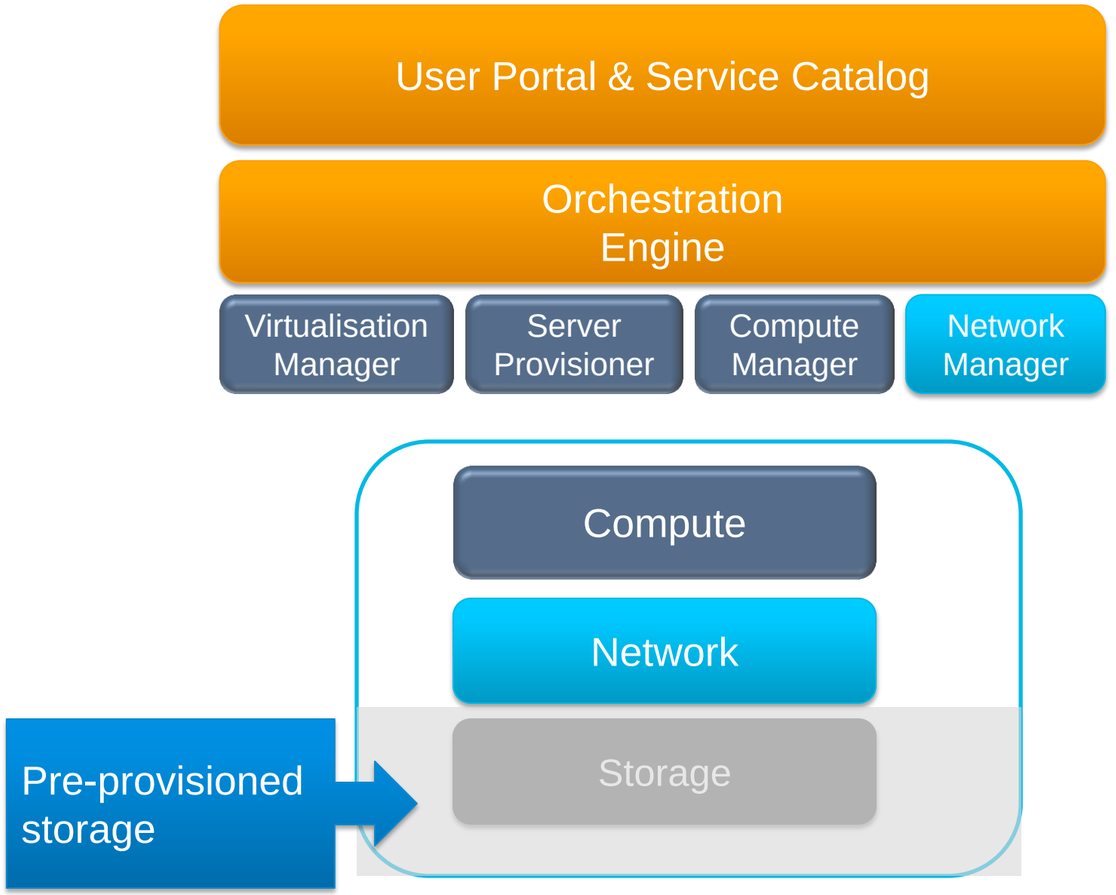
Cisco IAC Orchestration Framework



Cisco IAC on VMDC

Cisco IAC - Compute and Network provisioning

- Availability: Now with Cisco IAC 3.1
- Use Case: Enterprise Private and SP Public Cloud
- Self service provisioning of VMs, Physical Servers and Network
- Tenant traffic will be segregated over a VMDC architecture
- Multi-tenant support
- Storage has to be manually configured (supported in later releases)



Securing Access to Cloud Services

Secure Services Access

USER

- Identify device
- Identify user
- Secure device

Server

- Identify process
- Identify server
- Secure server

- Secure tunnel:
  - User to app
  - Server to service

Application* Protection

- Network security:
  - Firewall
  - IPS
  - Anti-X
  - DDoS protection
- Logical security:
  - App/Svc brokering / entitlement
  - Coarse / granular app control
  - WAF
  - Application testing / audit
  - Attack simulation / PenTest

- SaaS
- SaaS 3rd party (plugin, bespoke)
- IaaS/PaaS (own apps)

* Application types: Web, native, VDI

Information Security

- Data in flight
- Data at rest
- Encryption / Key Mgt
- DLP

- Messages/attach
- Files / unstructured data
- Forms / structured data

- SIO
- Threat Defence
- Anomaly

Web Security (slide from Cisco Live 2012)

"ScanSafe and Meraki signal how serious Cisco is about the cloud, expect exciting new things in 2013…"

Summary

Cloud Security Recommendations

For Cloud Services Providers

Actions

- Create transparency and awareness to address customer security concerns
- Create a strong security posture
- Offer security services in the services portfolio
- Use Cisco® cloud security checklist to deliver cloud security

Benefits

- Business enablement
- Liability and loss reduction
- Profit growth
- Reduced time to market and CapEx

Cloud Security Recommendations

For Private and Hybrid Cloud Owners and Practitioners

Actions

- Include cloud security in corporate governance
- Build cloud security into cloud architecture
- Implement accountability and review cycle
- Use Cisco® cloud security checklist to implement cloud security

Benefits

- User awareness and management support
- In-depth and integrated cloud security to mitigate threats
- Process-oriented diligence and improvement

…. Tying Products to Solution…

Secure Cloud Infrastructure

- Virtualised Multi tenant Data Centre Architecture
- Cisco ASA 5585; ASA SM; ASA1000V
- Cisco Nexus® 1000V switch
- Cisco VSG and ASA 1000V

Cloud Security Services

- Cisco ScanSafe Web Security and Filtering
- Cisco IronPort® Cloud, Managed, and Hybrid Email Security
- Cisco SIO:
  - Cisco SensorBase™
  - Threat Operations Centre
  - Dynamic updates

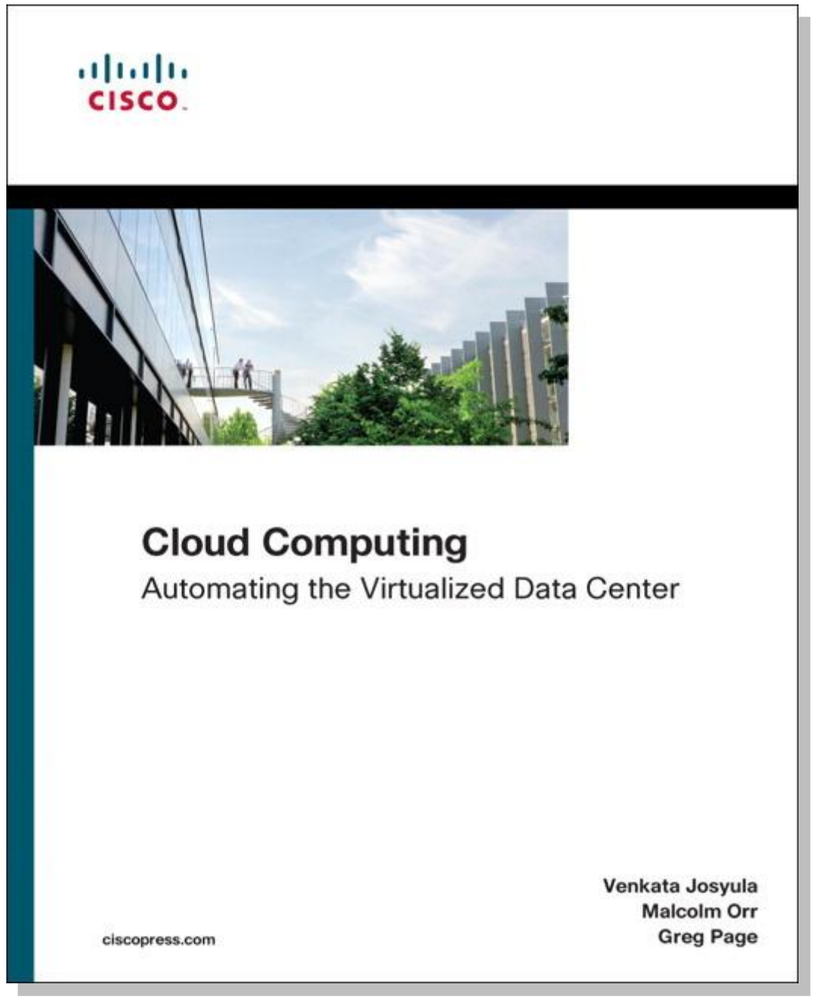
Secure Cloud Access

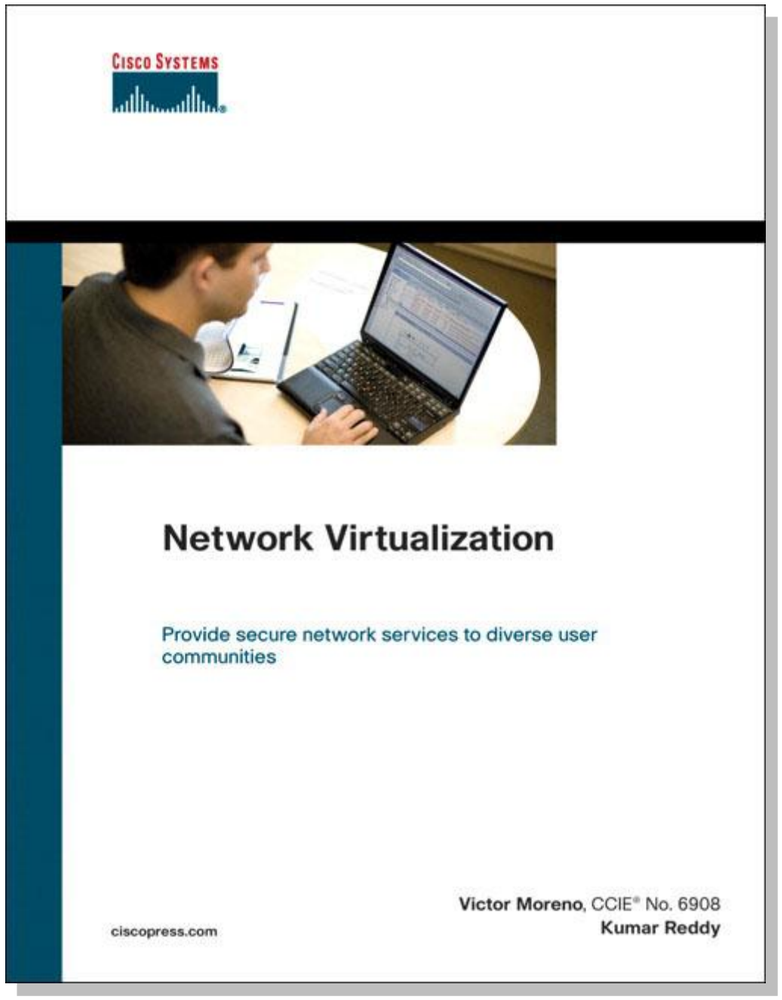
- Secure SaaS access
- Cisco AnyConnect™
- Cisco TrustSec®
- Cisco Identity Services Engine
- VPN

Cloud Thoughts

- Build a secure, virtualised, multi-tenant Data Centre architecture to deploy your services on
  - Do not sacrifice security in order to achieve efficiency with virtualisation!
  - Continue using the Security Best Practices on all layers (L2, L3, L4)
  - Deploy Security monitoring tools which can monitor and report on everything which happens
- Build or buy a tool which can configure and manage all the components in a dynamic, hands-off manner
- Make sure your solution is and will continue to be compliant with your Security Policy, user SLA's, PCI, and all the other requirements

Recommended Reading for BRKSEC-2009





Resources

- Virtualied Multi-Tenant Data Center (VMDC): www.cisco.com/go/vmdc
- Cisco CSR 1000V: http://www.cisco.com/go/cloudrouter/

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm

Cisco live! 365

Don’t forget to activate your Cisco Live 365 account for access to all session material, communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.
www.ciscoliveaustralia.com/portal/login.ww

Cisco live!