CISCO

TOMORROW
starts here.

Cisco*live!*

Securing My SP Network

BRKSEC-2004

Michael Geller – Principal Engineer, CTAO

#clmel

Rules of the Game!

- Silence your phone, pda, pager, mp3 player…
- At CiscoLive! your evaluation is extremely important
- Please remember to wear your badge at all times
- Please visit the World of Solutions

- PLEASE! Ask questions any time

Meet the Expert

- To make the most of your time at Networkers at Cisco Live 2015, schedule a Face-to-Face Meeting with top Cisco Engineers.
- Designed to provide a "big picture" perspective as well as "in-depth" technology discussions, these face-to-face meetings will provide fascinating dialogue and a wealth of valuable insights and ideas.
- Visit the Meeting Centre reception desk located in the World of Solutions.

Prerequisites

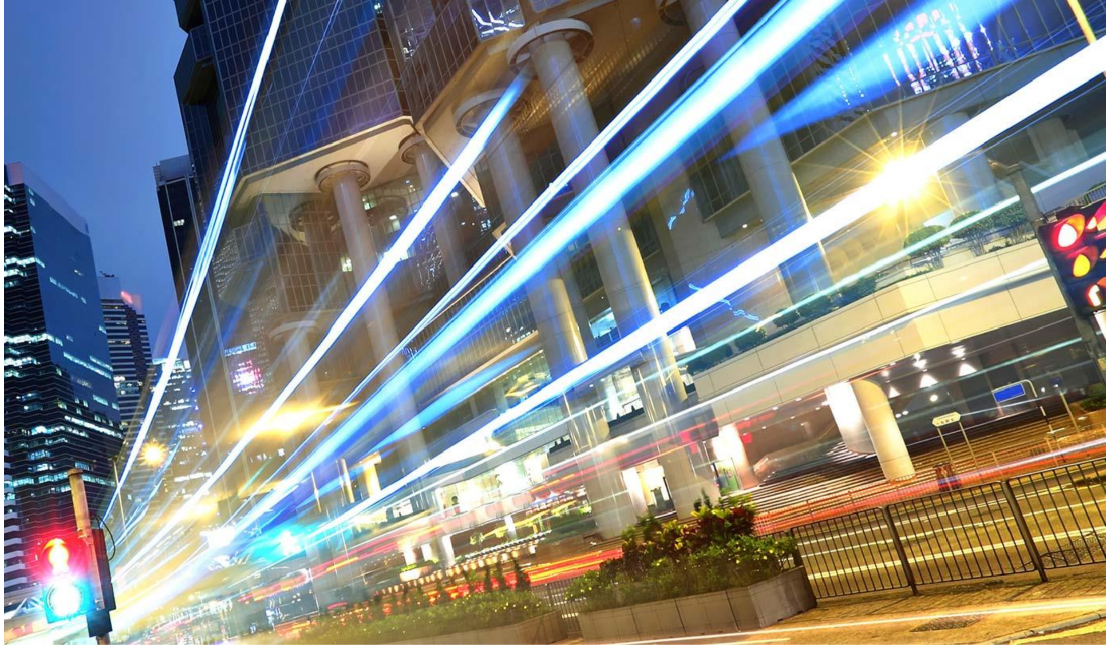
- Before attending this session, familiarity with basic security concepts as they apply to networks and business outcomes
- Some familiarity with Virtualisation, SDN and NfV is helpful, but not mandatory
- Thoughts about how security fits in the way you run your business today and the impact of the cloud

Objectives

- This session targets hosted security services for Enterprises and Service Providers
- Understand the impact of orchestration & automation for hosted security
- Cool applications of elastic security services delivered from the cloud
- Performance and scalability considerations
- Security services with NfV and SDN
- Future thinking applications of security from the Cloud to YOUR network

Agenda

- Introduction
- The Hosted Security Service Architecture
  - Architecture
  - HSS: Architecture and Demonstration
  - CloudVPN: Architecture and Demonstration
- Conclusion



IT Transformation

IT/SECURITY TEAM

Constant Evolution of Threats

More devices and more apps mean the attack surface has increased, and attack tools are evolving, too

Device Explosion

The hardware we use has never changed so fast

Expected Ongoing IT Productivity Gains

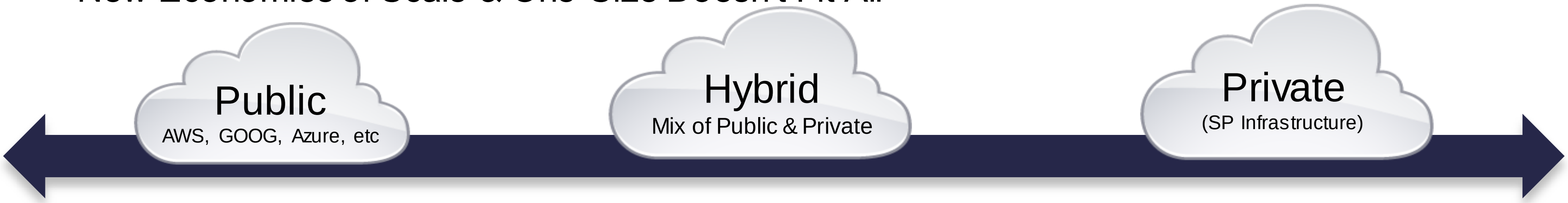
Do more with less

End-User-Focused Application Explosion

Users will get stuff done any way they can

End Customer Expectations

- ✓ On-Demand & Real Time Customer Requirements coupled with amazing & custom user experiences
- ✓ Multiple Applications, No Limit to “Environment” or Cloud
- ✓ New Consumption Models & Multiple Roles Consuming Cloud Differently; Products, Solutions & Application types (Developer -> IT -> Business User)
- ✓ Cross-Environment Requirements: Public, Private, Hybrid for App Development, Delivery/Deployment, Operation & Maintenance, Add-Ons & Customisation
- ✓ New Economies of Scale & One Size Doesn’t Fit All



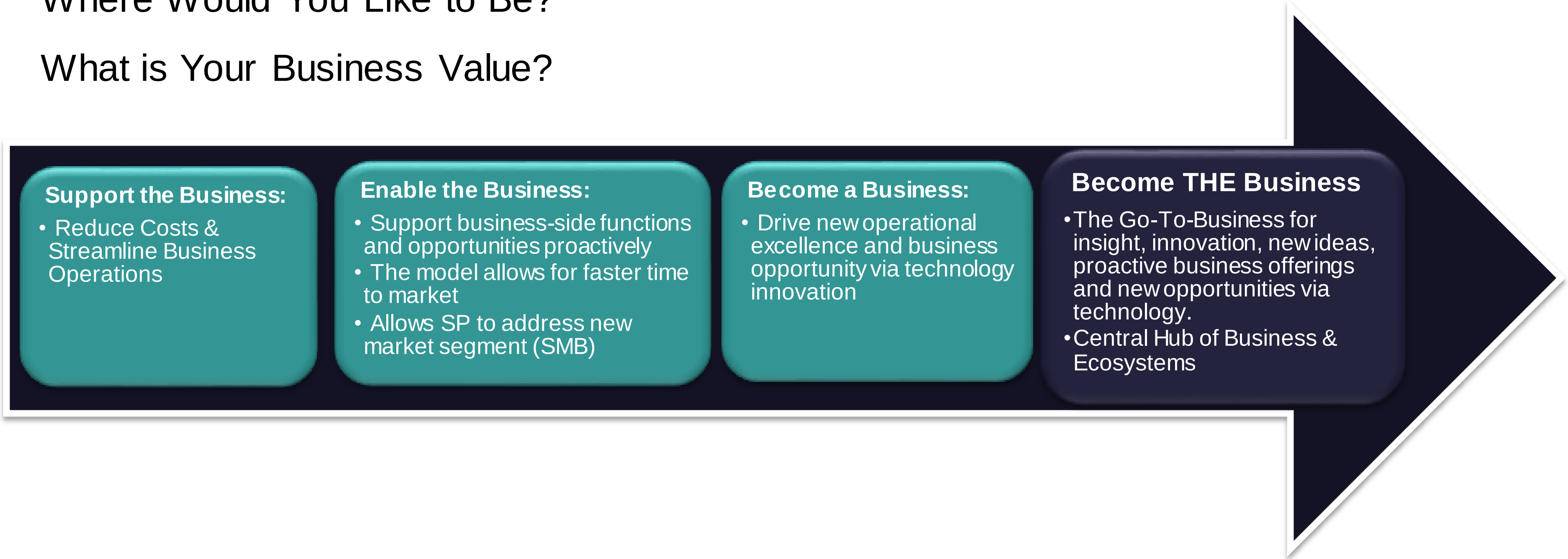
Seamless End-to-End Experiences, Cross Workload Size & Type
Required Regardless of App, Service or Environment; Secure Flexibility Critical Requirement

Transformations in Business & Models for Success

Delivering on User Experience Inside & Outside of Your Business Ecosystem

Where Would You Like to Be?

What is Your Business Value?



Support the Business:

- Reduce Costs & Streamline Business Operations

Enable the Business:

- Support business-side functions and opportunities proactively
- The model allows for faster time to market
- Allows SP to address new market segment (SMB)

Become a Business:

- Drive new operational excellence and business opportunity via technology innovation

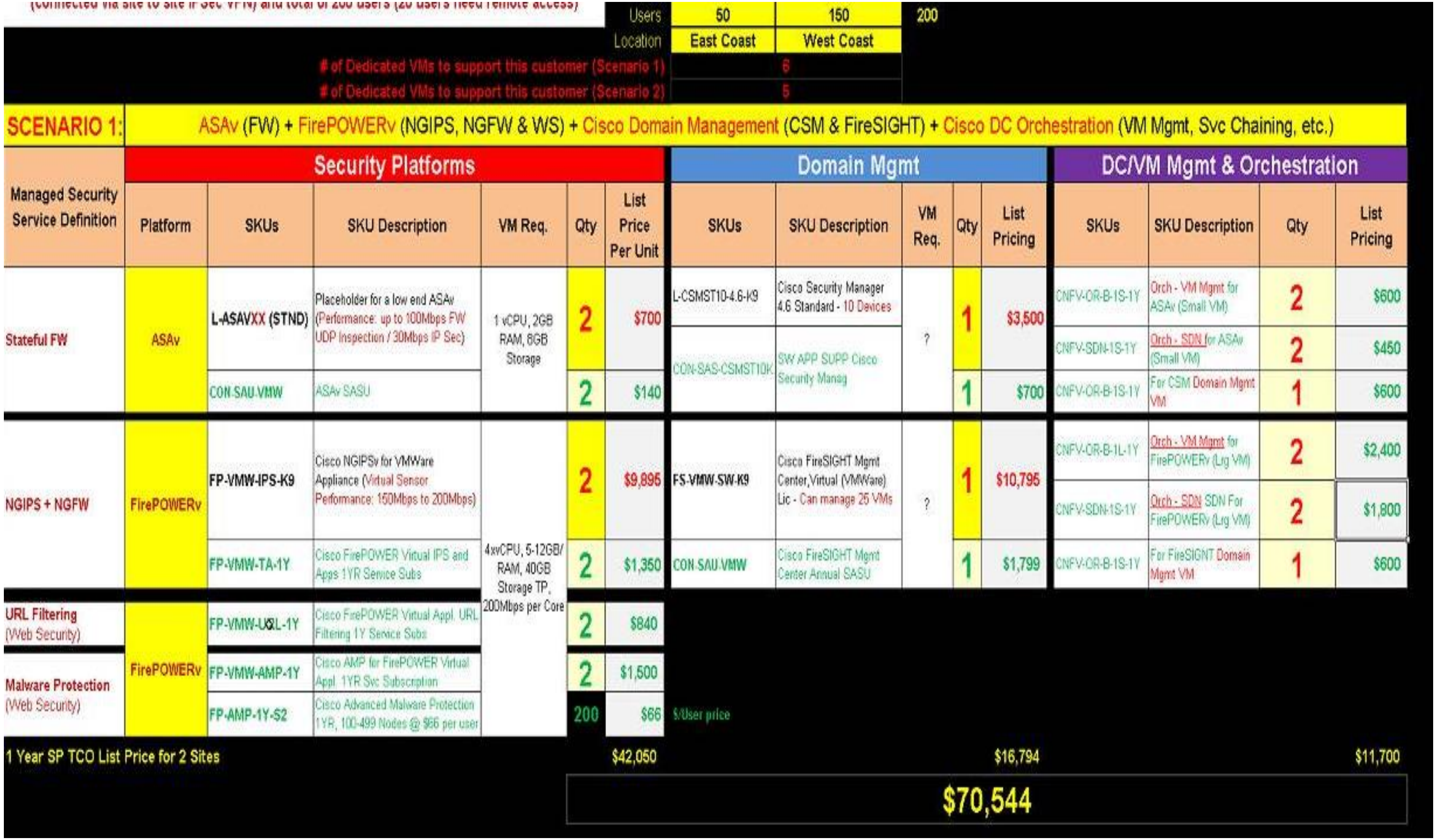
Become THE Business

- The Go-To-Business for insight, innovation, new ideas, proactive business offerings and new opportunities via technology.
- Central Hub of Business & Ecosystems

Technology + Business Driving New Markets & Revenue

Your Business is the Required Central Hub

Business Case Modelling to Ensure Profitable Business



(connected via site to site IPSec VPN) and total of 200 users (20 users need remote access)

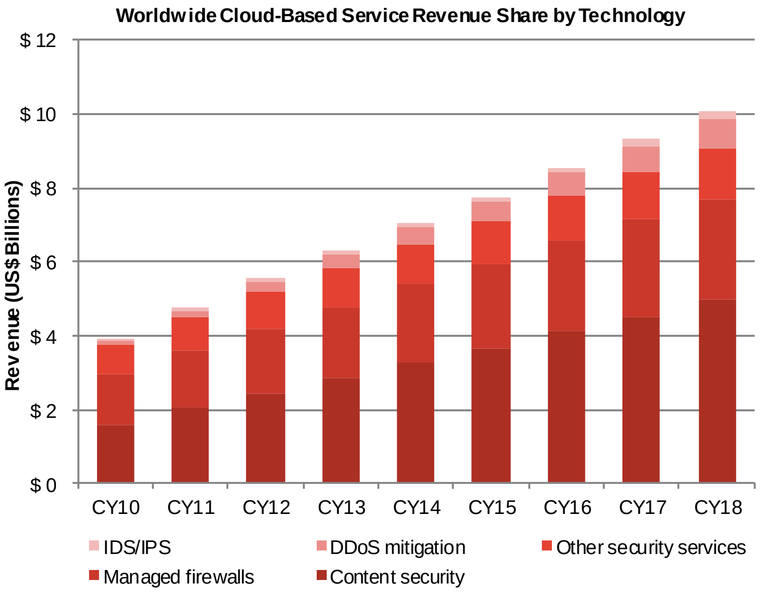
Users	50	150	200
Location	East Coast	West Coast	
# of Dedicated VMs to support this customer (Scenario 1)	6		
# of Dedicated VMs to support this customer (Scenario 2)	5		

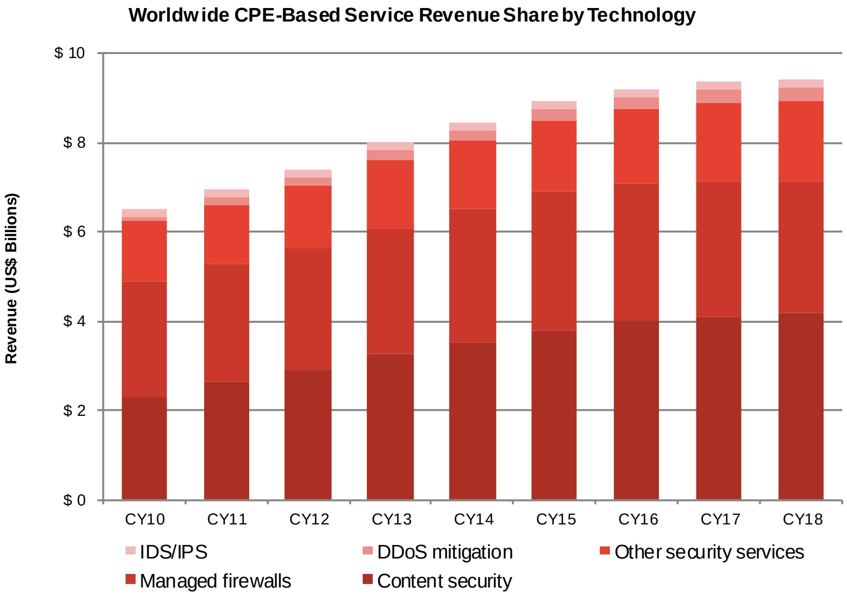
SCENARIO 1: ASAv (FW) + FirePOWERv (NGIPS, NGFW & WS) + Cisco Domain Management (CSM & FireSIGHT) + Cisco DC Orchestration (VM Mgmt, Svc Chaining, etc.)

	Security Platforms						Domain Mgmt					DC/VM Mgmt & Orchestration			
Managed Security Service Definition	Platform	SKUs	SKU Description	VM Req.	Qty	List Price Per Unit	SKUs	SKU Description	VM Req.	Qty	List Pricing	SKUs	SKU Description	Qty	List Pricing
Stateful FW	ASAv	L-ASAVXX (STND)	Placeholder for a low end ASAv (Performance: up to 100Mbps FW UDP Inspection / 30Mbps IP Sec)	1 vCPU, 2GB RAM, 8GB Storage	2	$700	L-CSMST10-4.6-K9	Cisco Security Manager 4.6 Standard - 10 Devices	?	1	$3,500	CNFV-OR-B-1S-1Y	Orch - VM Mgmt for ASAv (Small VM)	2	$600
							CON-SAS-CSMST10K	SW APP SUPP Cisco Security Manag				CNFV-SDN-1S-1Y	Orch - SDN for ASAv (Small VM)	2	$450
		CON-SAU-VMW	ASAv SASU		2	$140				1	$700	CNFV-OR-B-1S-1Y	For CSM Domain Mgmt VM	1	$600
NGIPS + NGFW	FirePOWERv	FP-VMW-IPS-K9	Cisco NGIPSv for VMWare Appliance (Virtual Sensor Performance: 150Mbps to 200Mbps)	4xvCPU, 5-12GB/ RAM, 40GB Storage TP, 200Mbps per Core	2	$9,895	FS-VMW-SW-K9	Cisco FireSIGHT Mgmt Center,Virtual (VMWare) Lic - Can manage 25 VMs	?	1	$10,795	CNFV-OR-B-1L-1Y	Orch - VM Mgmt for FirePOWERv (Lrg VM)	2	$2,400
												CNFV-SDN-1S-1Y	Orch - SDN SDN For FirePOWERv (Lrg VM)	2	$1,800
		FP-VMW-TA-1Y	Cisco FirePOWER Virtual IPS and Apps 1YR Service Subs		2	$1,350	CON-SAU-VMW	Cisco FireSIGHT Mgmt Center Annual SASU		1	$1,799	CNFV-OR-B-1S-1Y	For FireSIGNT Domain Mgmt VM	1	$600
URL Filtering (Web Security)	FirePOWERv	FP-VMW-URL-1Y	Cisco FirePOWER Virtual Appl. URL Filtering 1Y Service Subs		2	$840									
Malware Protection (Web Security)		FP-VMW-AMP-1Y	Cisco AMP for FirePOWER Virtual Appl. 1YR Svc Subscription		2	$1,500									
		FP-AMP-1Y-S2	Cisco Advanced Malware Protection 1YR, 100-499 Nodes @ $66 per user		200	$66	$/User price								
1 Year SP TCO List Price for 2 Sites						$42,050					$16,794				$11,700
					$70,544										

Market Opportunity

Cloud Service Delivery Shows Higher Growth, but CPE Based Still Growing

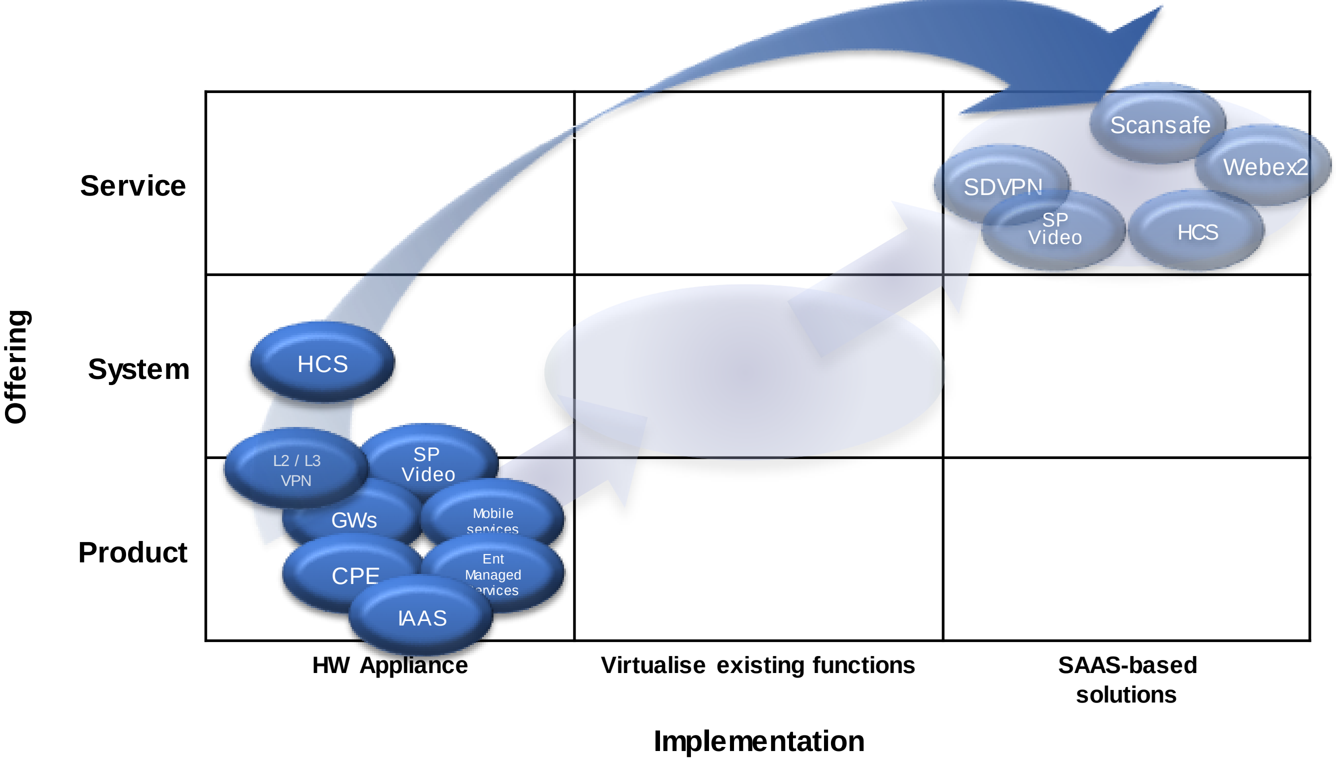




INFONETICS RESEARCH **© Infonetics Research: *Cloud and CPE Managed Security Service Market Size and Forecasts*, March 2014**

Transition to All-virtualised Services?

- Drivers:
- **Reducing total OpEx and CapEx**
- Increased service velocity and agility
- Increasing revenue



Offering

Service

System

Product

HCS

L2 / L3 VPN

SP Video

GWs

Mobile services

CPE

Ent Managed services

IAAS

Scansafe

Webex2

SDVPN

SP Video

HCS

HW Appliance

Virtualise existing functions

SAAS-based solutions

Implementation

Cisco Security as a Service Solutions

Service Provider Virtual Private Cloud

Hosted Security Solution & CloudVPN

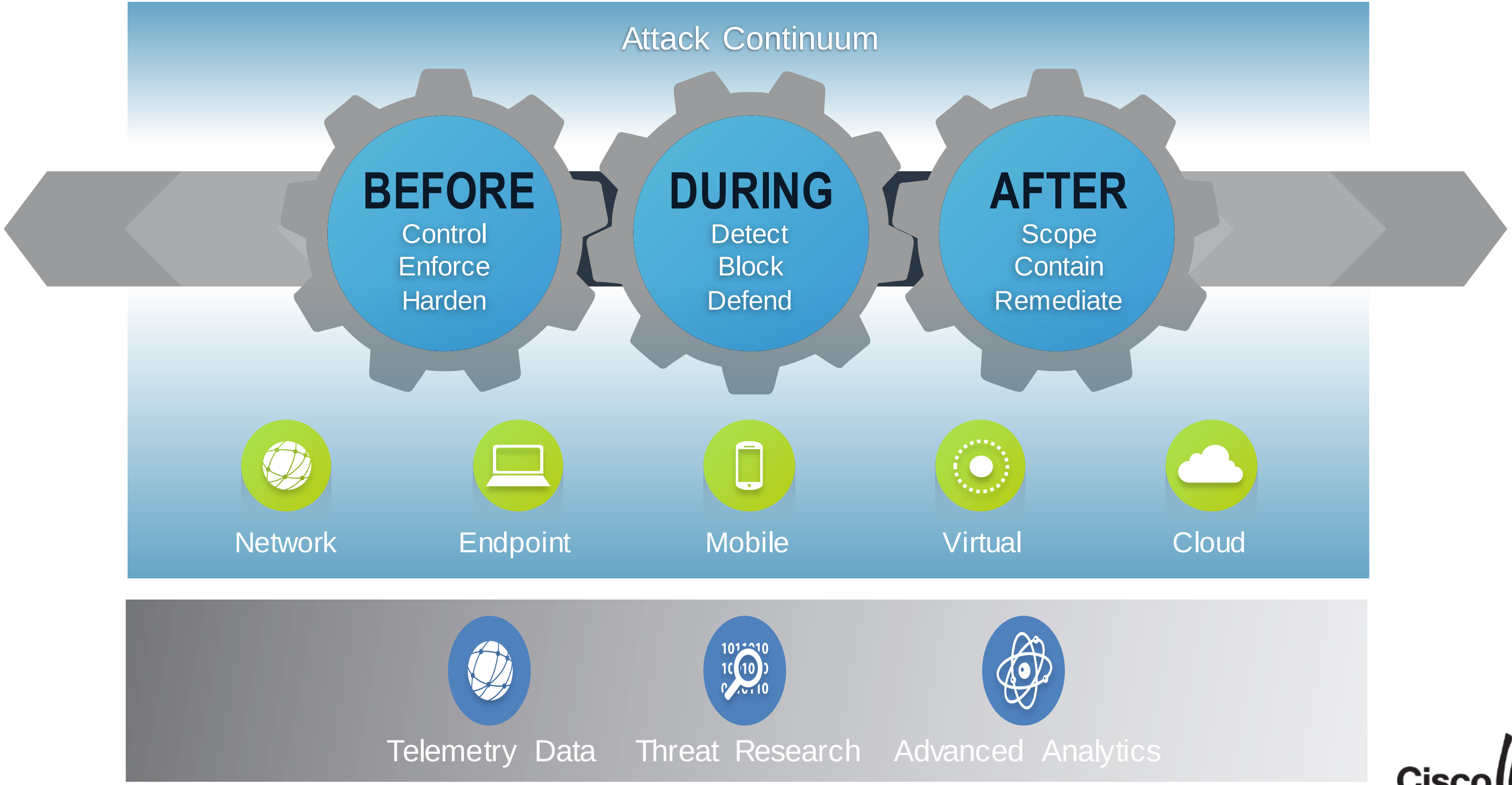
SP-Hosted Firewall, VPN, IPS, Email, and Web Services

Turnkey Public Cloud

Cisco Managed Security Cloud

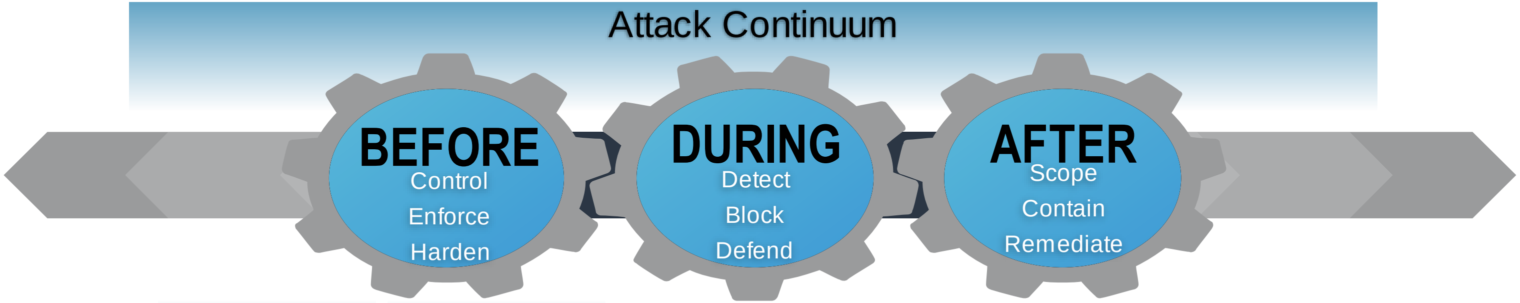
Cisco or SP-Hosted, Cisco-Run Web Security Services

The New Security Model



Managing The Threat Lifecycle

Protecting the Infrastructure and Offering Elastic Managed Services



Firewall | VPN | NGIPS | Advanced Malware Protection

NGFW | UTM | Web Security | Network Behaviour Analysis

NAC + Identity Services | Email Security | Forensic Analytics

DDoS Visibility/Mitigation Services

Visibility, Context, Autonomics and BCPs

Orchestration

CloudVPN
Cloud Services Orchestration

Real Time application of the right service, in the right place, at the right time

Quantum WAVE
WAN Orchestration

Real time topology and service health information

HSS
UBIqube – MS Activator

Security Domain Management

Firewall-aaS Tiers Example

BEFORE

DURING

AFTER

Feature Category	Service Tiers		
	Bronze	Silver	Gold
NAT Address Translation	✓	✓	✓
Stateful Inspection	✓	✓	✓
High Availability		✓	✓
Advanced Management			✓

✓ Included

Firewall-aaS Tiers Example

Reference Slide

Category	Feature	Service Tiers		
		Bronze	Silver	Gold
NAT Address Translation	NAT / PAT	✓	✓	✓
Stateful Inspection	L3 firewall	✓	✓	✓
	Transparent firewall		…	…
	Proxy authentication		✓	✓
	Application hosting private zone		…	…
	Application control (IM, peer to peer)		…	…
	Voice security support		…	…
High availability	Within SP data centre		✓	✓
	Between SP data centres		…	…
Management	Customer self service portal		✓	✓
	Streamlined management	✓		
	Auto generated reporting	✓	✓	✓
	Custom reporting			✓
	Data log retention (1 month)	✓	✓	✓
	Extended data log retention (> 1 month)			✓

✓ Included

… Option

VPNaaS Tiers Example

Feature Category	Service Tiers		
	Bronze	Silver	Gold
Customer site to Cloud IPSec VPN service	✓	✓	✓
Remote Access VPN	✓	✓	✓
High Availability		✓	✓
Advanced Management			✓

✓ Included

VPNaaS Tiers Example

Reference Slide

Category	Feature	Service Tiers		
		Bronze	Silver	Gold
Customer site to Cloud IPsec VPN service	Support for multiple crypto policies (DES, 3DES, AES …)	✓	✓	✓
	Pre-shared key VPN authentication	✓	✓	✓
	Digital certificate VPN authentication		⋯	⋯
	Multiple class of services / traffic prioritization policies		✓	✓
Remote access VPN	IPSec based remote access VPN	✓	✓	✓
	Client-less SSL remote access VPN	✓	✓	✓
	Client-based SSL remote access VPN		⋯	⋯
	Authentication integration with enterprise's radius, LDAP, AD servers		⋯	⋯
	Basis authentication (username and password based)	✓	✓	✓
	Strong authentication / token based authentication		⋯	⋯
	Digital certificate based authentication		⋯	⋯
High availability	Active / Passive within SP data centre		✓	
	Active / Active within SP data centre			✓
	Active / Passive between SP data centre		⋯	
	Active / Active between SP data centre			⋯
Management	Customer self service portal		✓	✓
	Streamlined management	✓		
	Auto generated reporting	✓	✓	✓
	Custom reporting			✓
	Data log retention (1 month)	✓	✓	✓
	Extended data log retention (> 1 month)			✓

✓ Included

⋯ Option

Web Security-aaS Tiers Example

Feature Category	Service Tiers		
	Bronze	Silver	Gold
Real Time Threat Protection Services	✓	✓	✓
Acceptable Use Services	✓	✓	✓
Policy Control		✓	✓
High Availability		✓	✓
Advanced Management			✓

✓ Included

Web Security-aaS Tiers Example

Reference Slide

Category	Feature	Service Tiers		
		Bronze	Silver	Gold
Real time threat protection services	Web reputation filtering	✓	✓	✓
	Malware scanning	✓	✓	✓
Acceptable use services	Web URL monitoring by category		✓	✓
	Web URL filtering (blocking)		···	···
	Web application monitoring			✓
	Web application control			···
	SaaS access control			···
	Transparent user authentication		···	···
	Advanced Malware Protection			✓
Policy control	Granular access and control policies			✓
	Remote access user control policies		···	···
High availability	Within SP data centre		✓	✓
	Between SP data centres		···	···
Management	Customer self service portal		✓	✓
	Streamlined management	✓	✓	✓
	Auto generated reporting			✓
	Custom reporting			✓
	Data log retention (1 month)	✓	✓	✓
	Extended data log retention (> 1 month)		···	···

✓	Included
···	Option

Email Security-aaS Tiers Example

Feature Category	Service Tiers		
	Bronze	Silver	Gold
Inbound Email Protection	✓	✓	✓
Outbound Email Protection	✓	✓	✓
Policy control		✓	✓
High availability		✓	✓
Advanced Management			✓

✓ Included

Email Security-aaS Tiers Example

Reference Slide

Category	Feature	Service Tiers		
		Bronze	Silver	Gold
Inbound email protection	Reputation scoring and SMTP blocking	✓	✓	✓
	Anti-spam	✓	✓	✓
	Outbreak filters, Sophos anti-virus		✓	✓
	Inbound email content filtering			✓
	Quarantine		…	…
	Advanced Malware Protection			✓
Outbound email protection	Anti-virus			✓
	Outbound email content filtering			✓
	Integrated RSA data loss prevention			…
	DLP RSA Enterprise Manager integration (Enterprise provided)			…
	Large volume			…
	Quarantine		…	…
Policy control	Granular policy control		…	…
	Roaming users protection		…	…
High availability	Within SP data centre		✓	✓
	Between SP data centres	✓		
Management	Self service portal		✓	✓
	Streamlined management	✓		
	Auto generated reporting	✓	✓	✓
	Custom reporting option			✓
	Data log retention (1 month)	✓	✓	✓
	Extended data log retention (> 1 month)		…	…

✓ Included

… Option

NGFW/IPSaaS Tiers Example

Feature Category	Service Tiers		
	Bronze	Silver	Gold
Application Visibility and Control (NGFW)	✓	✓	✓
Threat Protection (NGIPS)	✓	✓	✓
High Availability		✓	✓
Advanced Management			✓

✓ Included

NGFW/IPSaaS Tiers Example

Reference Slide

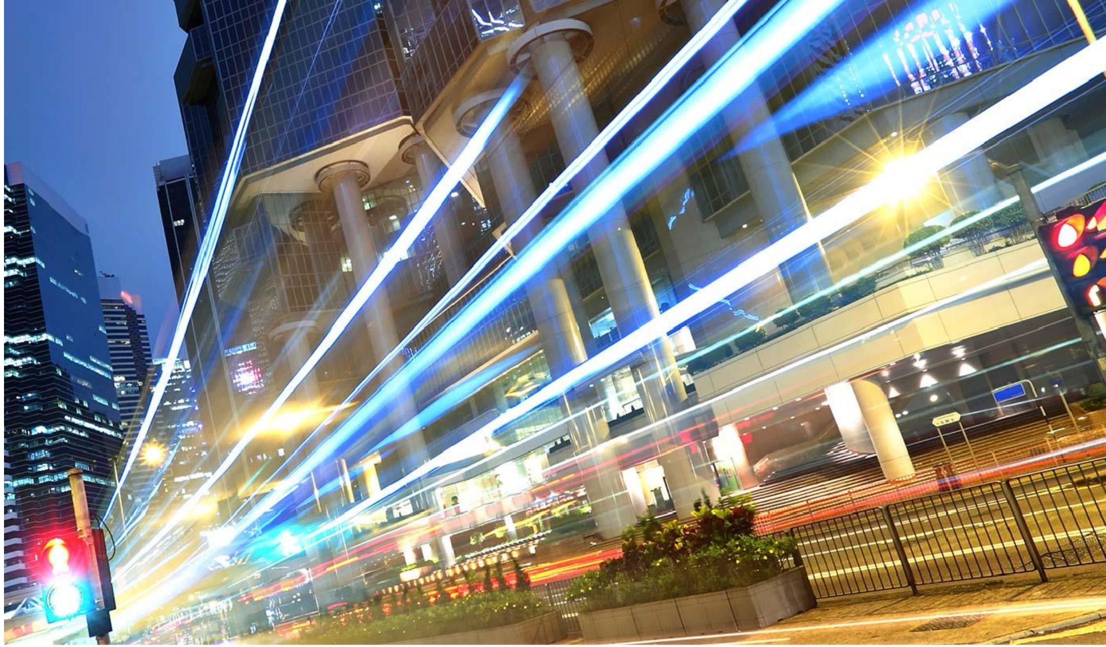
Category	Feature	Service Tiers		
		Bronze	Silver	Gold
Application Visibility and Control (NGFW)	Network, User and Application Discovery	✓	✓	✓
	Application Traffic filtering		✓	✓
	URL Filtering			✓
	File Blocking (block xyz file type)			✓
Threat Protection (NGIPS)	IPS Basic Threat Protection Services (SNORT signatures)	✓	✓	✓
	IPS premium security signatures and content	✓	✓	✓
	Security Intelligence Feeds			✓
	AMP (Advanced Malware Protection– disposition from the cloud/policy)			✓
High Availability	Configurable “fail open” – Appliance only			✓
	“Fastpath” & Trust Rules – Exclude/Include velocity			✓
Management	Streamline Management		✓	✓
	IPS signature update	✓	✓	✓
	Advanced/Custom Reporting		⋯	✓
	Automated Policy Tuning – Advanced/Custom Policy Tuning			✓
	Event Correlation – Customized Event Correlation Services		✓	✓
	Impact Analysis			✓

✓ Included

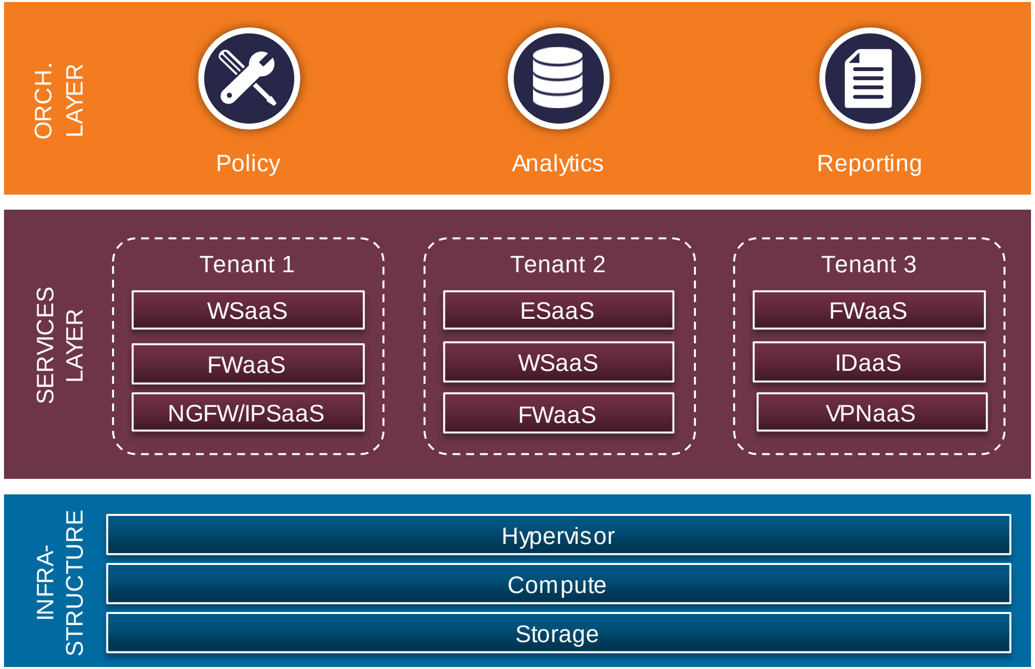
⋯ Option

Agenda

- Introduction
- The Hosted Security Service Architecture
  - Architecture
  - HSS: Architecture and Demonstration
  - CloudVPN: Architecture and Demonstration
- Conclusion



Hosted Security as a Service Architecture



Security Service Examples:

FWaaS – Firewall as a Service

VPNaaS – Virtual Private Networking as a Service

NGFW/IPSaaS – Next Generation Firewall and Intrusion Prevention System as a Service

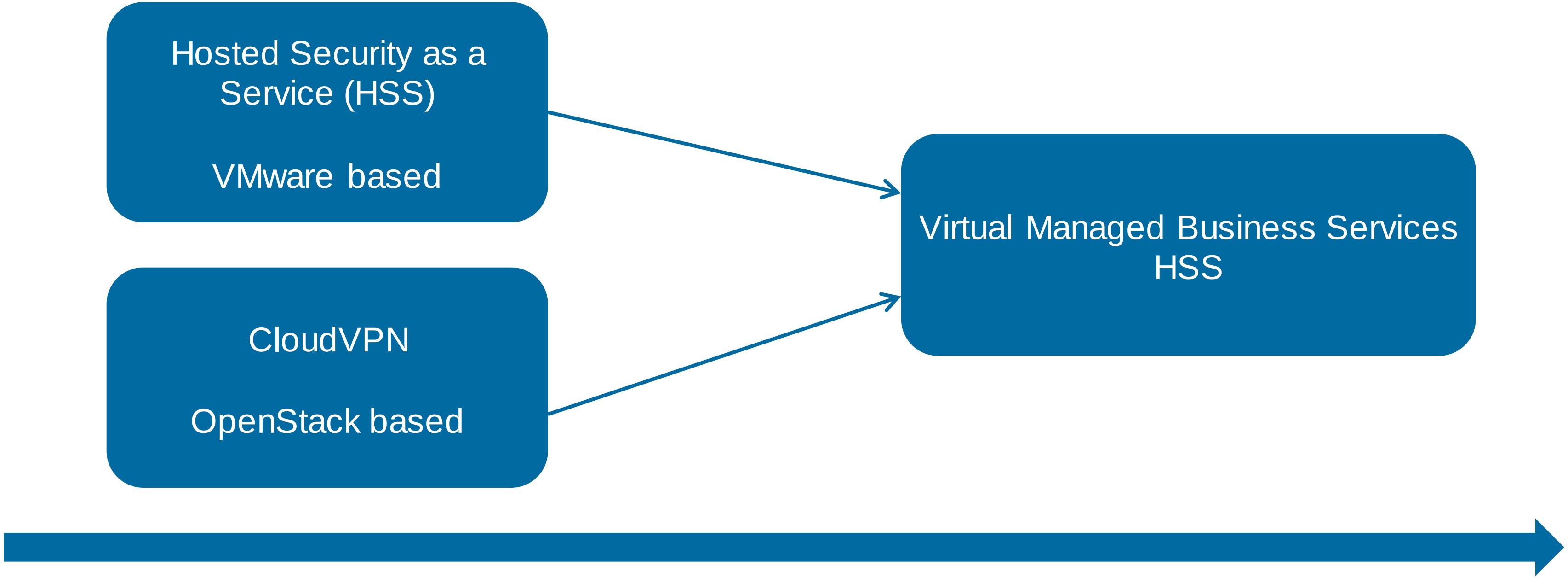
WSaaS – Web Security as a Service

ESaaS – Email Security as a Service

IDaaS – Identity as a Service

DDoSaaS – Distributed Denial of Service as a Service

Two Hosted Security as a Service Solutions Converging



Hosted Security as a Service (HSS)

VMware based

CloudVPN

OpenStack based

Virtual Managed Business Services HSS

Today

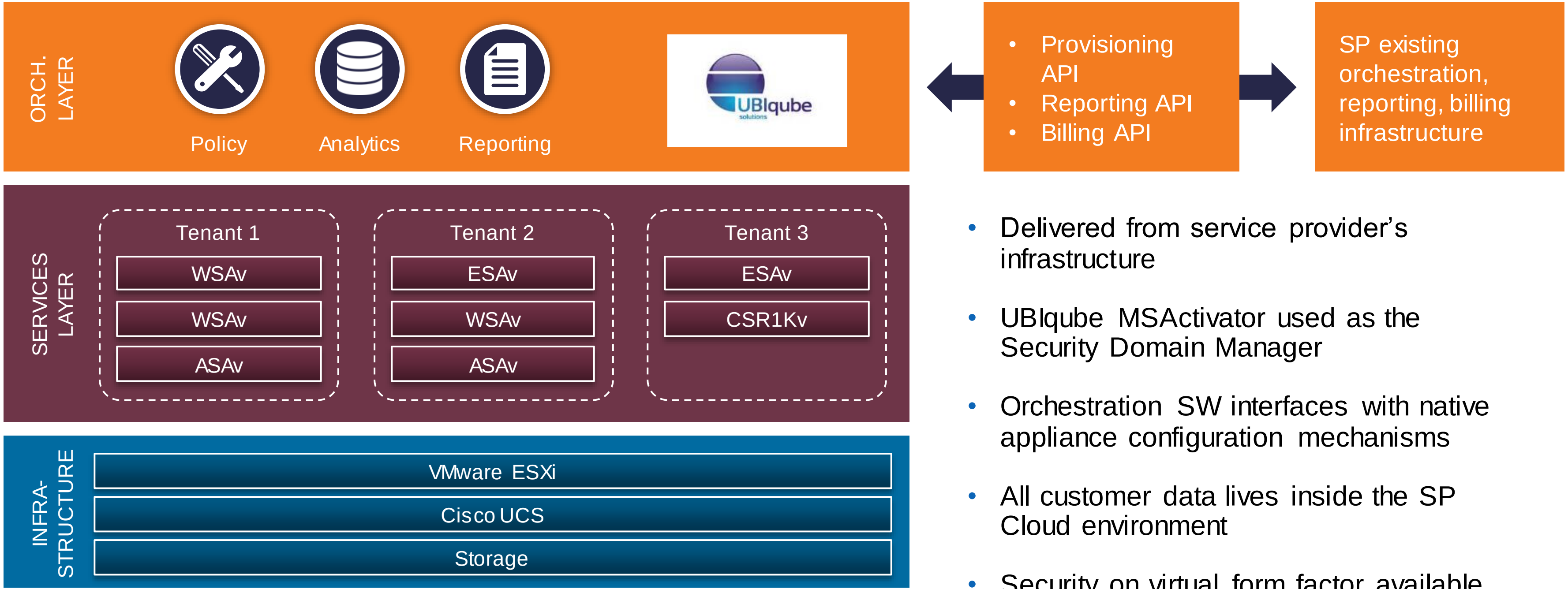
Future

Hosted Security as a Service

Hosted Security as a Service (HSS)

- Enables Cisco partners to deliver security services from their Cloud infrastructure or as a managed private cloud offering
- Cisco's virtual security appliance product (ESAV, WSAV, ASAV, …) and third party products
- Comprehensive management system using UBIqube as a security domain manager
  - Fulfillment
  - Assurance
  - Northbound API for integrating with Cloud Orchestration Solutions
- Solution supported with IaaS solution VMDC 2.3, testing with VSA 1.0 now
- Platform based on Cisco Unified Computing System (UCS)
- Flexible deployment models

HSS Architecture



ORCH. LAYER

Policy

Analytics

Reporting

UBIqube solutions

- Provisioning API
- Reporting API
- Billing API

SP existing orchestration, reporting, billing infrastructure

SERVICES LAYER

Tenant 1	Tenant 2	Tenant 3
WSAv	ESAv	ESAv
WSAv	WSAv	CSR1Kv
ASAv	ASAv	

INFRA-STRUCTURE

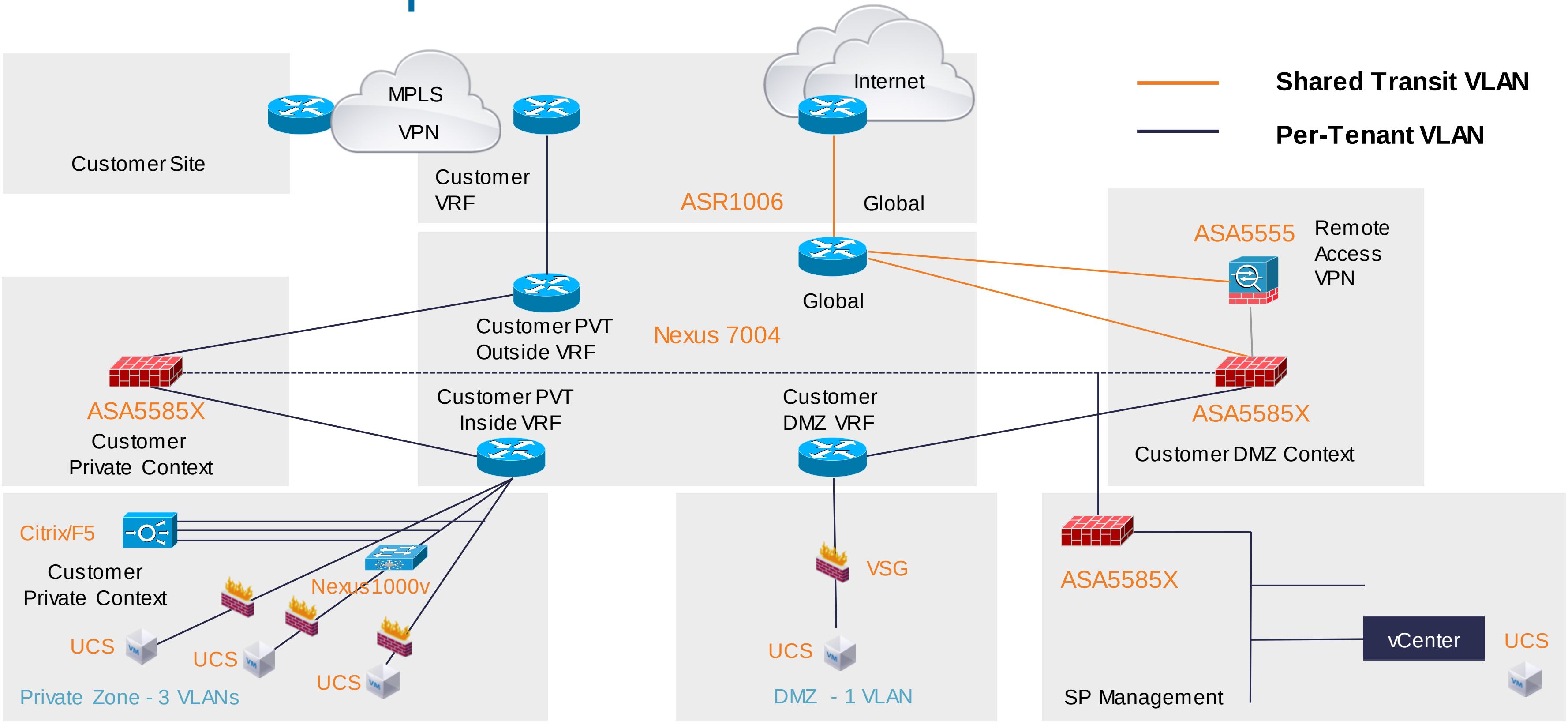
VMware ESXi

Cisco UCS

Storage

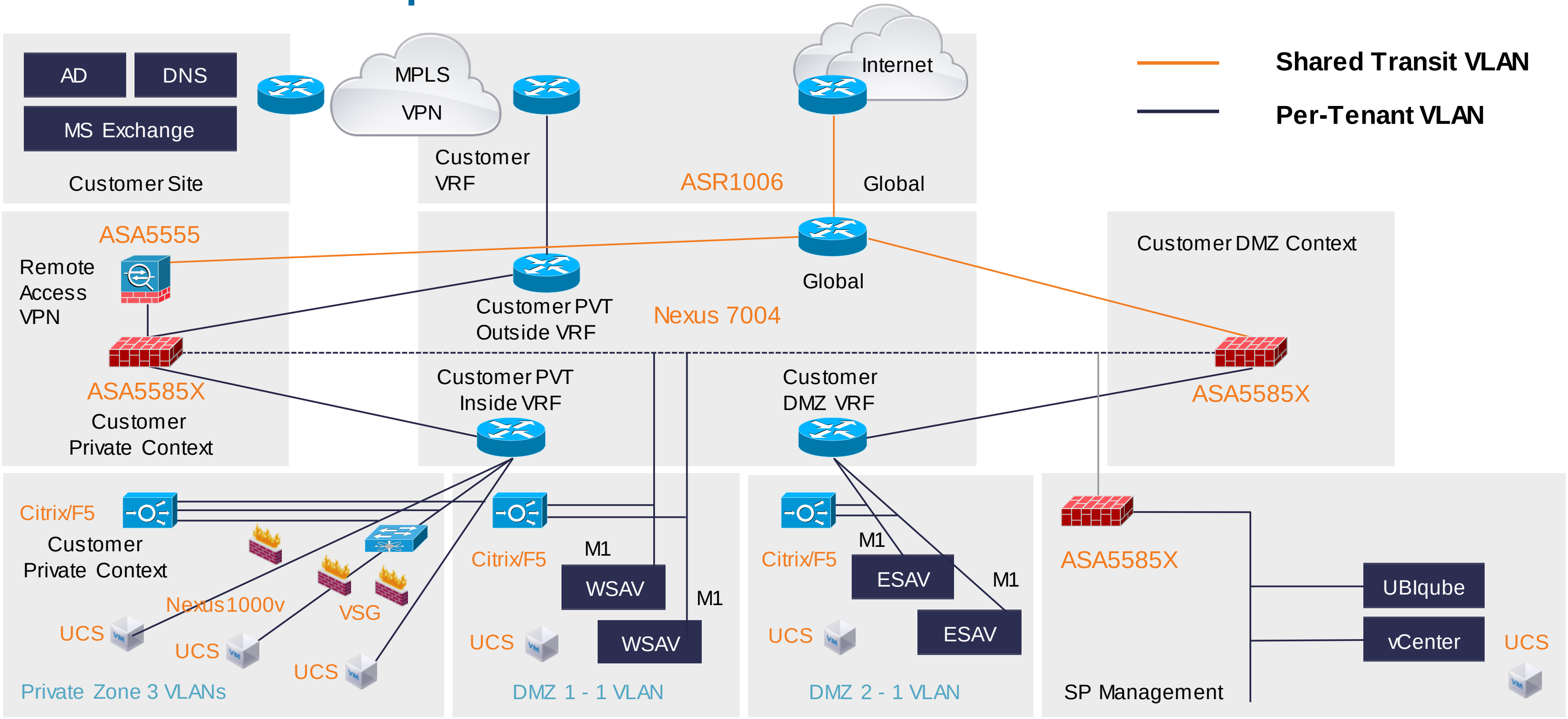
- Delivered from service provider’s infrastructure
- UBIqube MSActivator used as the Security Domain Manager
- Orchestration SW interfaces with native appliance configuration mechanisms
- All customer data lives inside the SP Cloud environment
- Security on virtual form factor available today

VMDC 2.3 Expanded Gold Container



*** Not showing redundant nodes**

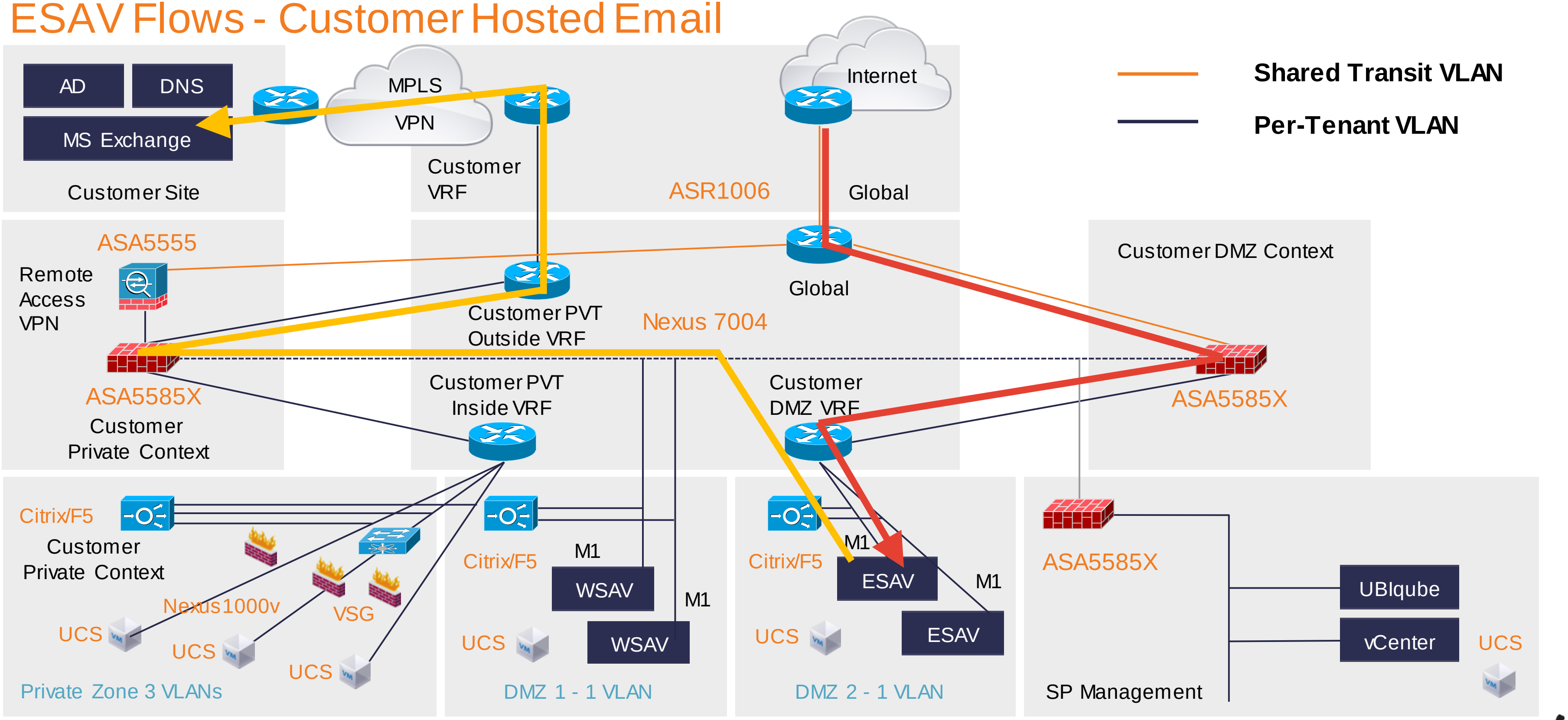
VMDC 2.3 Expanded Gold Container with HSS



*** Not showing redundant nodes**

VMDC 2.3 Expanded Gold Container with HSS

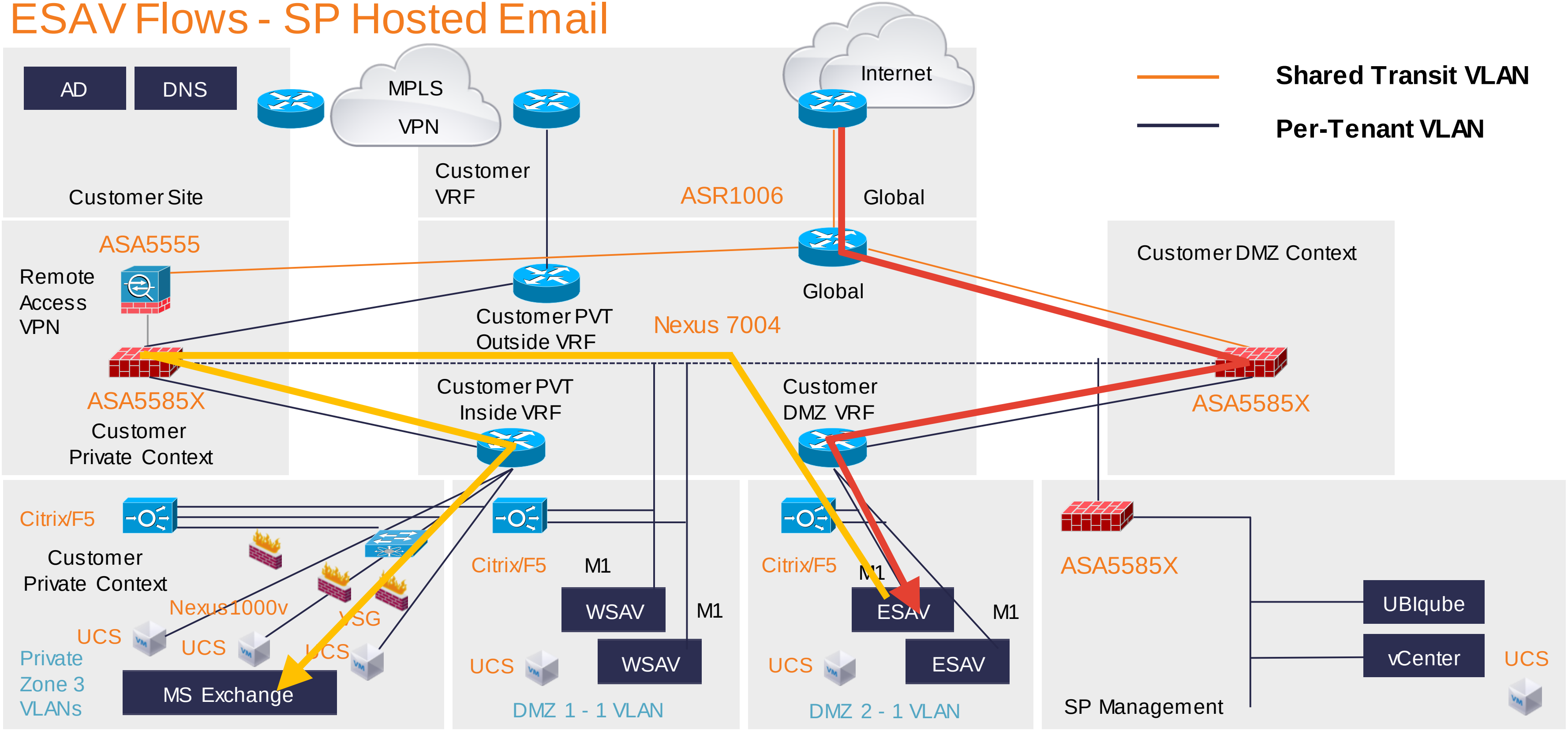
ESAV Flows - Customer Hosted Email



*** Not showing redundant nodes**

VMDC 2.3 Expanded Gold Container with HSS

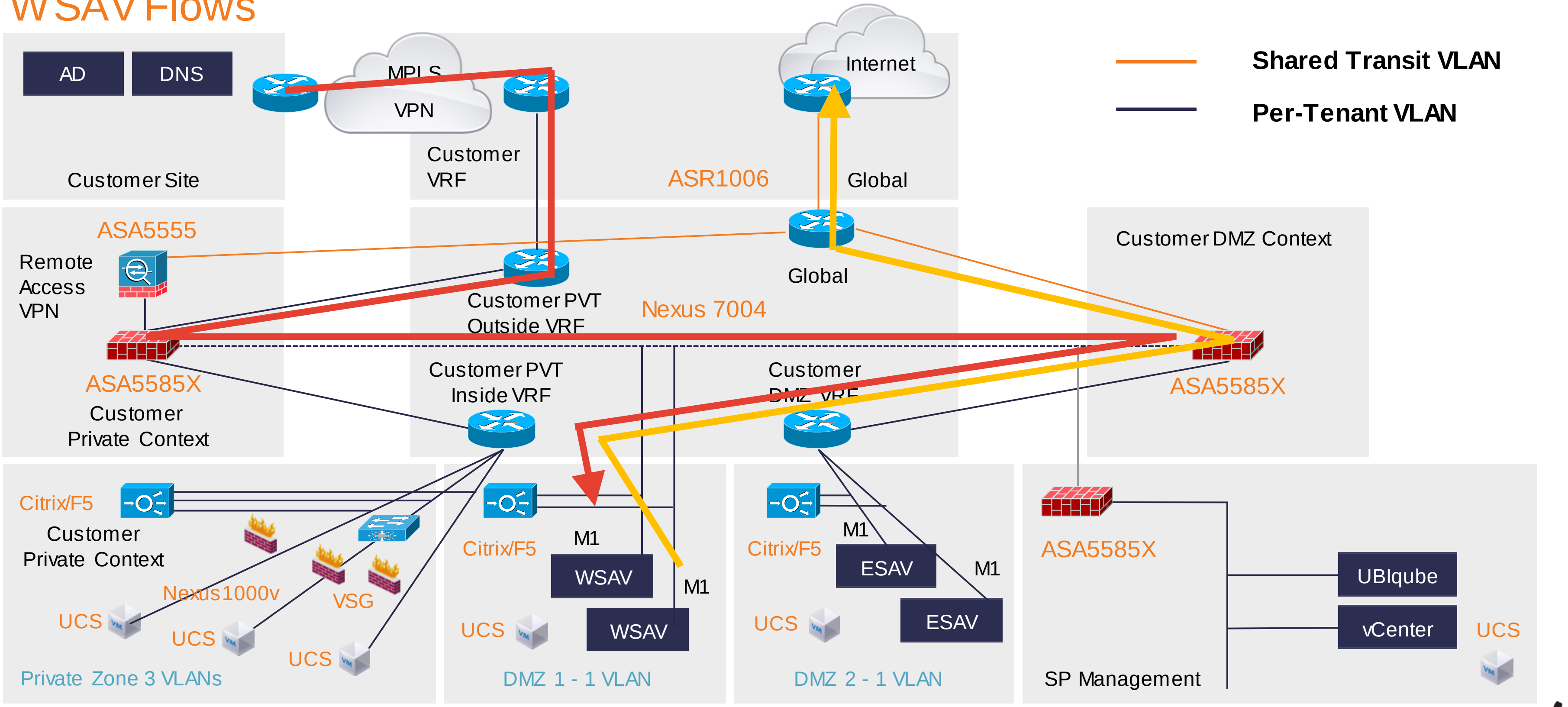
ESAV Flows - SP Hosted Email



*** Not showing redundant nodes**

VMDC 2.3 Expanded Gold Container with HSS

WSAV Flows



*** Not showing redundant nodes**

HSS Phase 1 Components

HSS Components	Version
VMDC Expanded Gold Container	2.3
WSAV	7.7.5
ESAV	8.0
UBIqube MSActivator	13.1
VMware vSphere	5.1
VMware vCenter	5.0

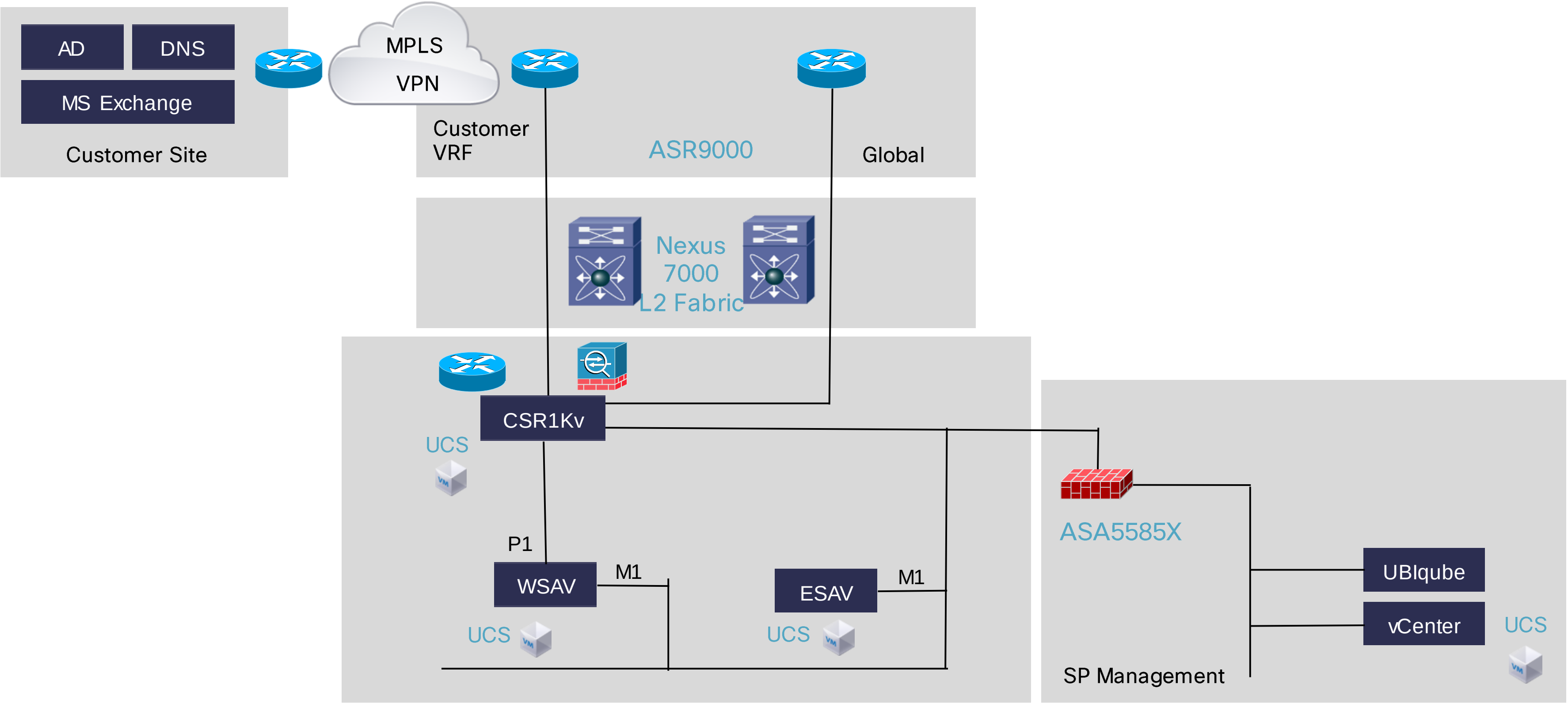
Cloud Orchestration Options	Version
Cisco Intelligent Automation for Cloud (CIAC)	4.0
BMC Cloud Lifecycle Manager	V3.1SP1

VMDC 2.3 Expanded Gold Container

VMDC 2.3 Component	Version	HSS Required/Recommended/Optional?
Unified Computing System (UCS)	2.0(4b)	UCS B or C required
ASR 1000	IOS XE 3.7.1S	Cisco 7600/ASR 1000/ASR 9000 recommended
ASA 5555-X (RA)	9.0.1	Recommended
ASA 5585-X (FW)	9.0.1	Recommended
Nexus 7000	NX-OS 6.1(3)	Recommended
Nexus 5548	NX-OS 5.2(1)N1(2)	Recommended
Nexus 1010	NX-OS 4.2(1)SP1(5.1)	Optional
Nexus 1000V	NX-OS 4.2(1)SV2(1.1)	Optional
Virtual Security Gateway (VSG)	NX-OS 4.2(1)VSG1(4.1)	Optional
Prime Network Management Controller (PNMC)	2.0(3f)	Optional
Citrix Netscaler VPX, SPX	10.1	Citrix or F5 recommended (if needed)
NetApp FAS	ONTAP 8.1.1	NetApp or EMC recommended

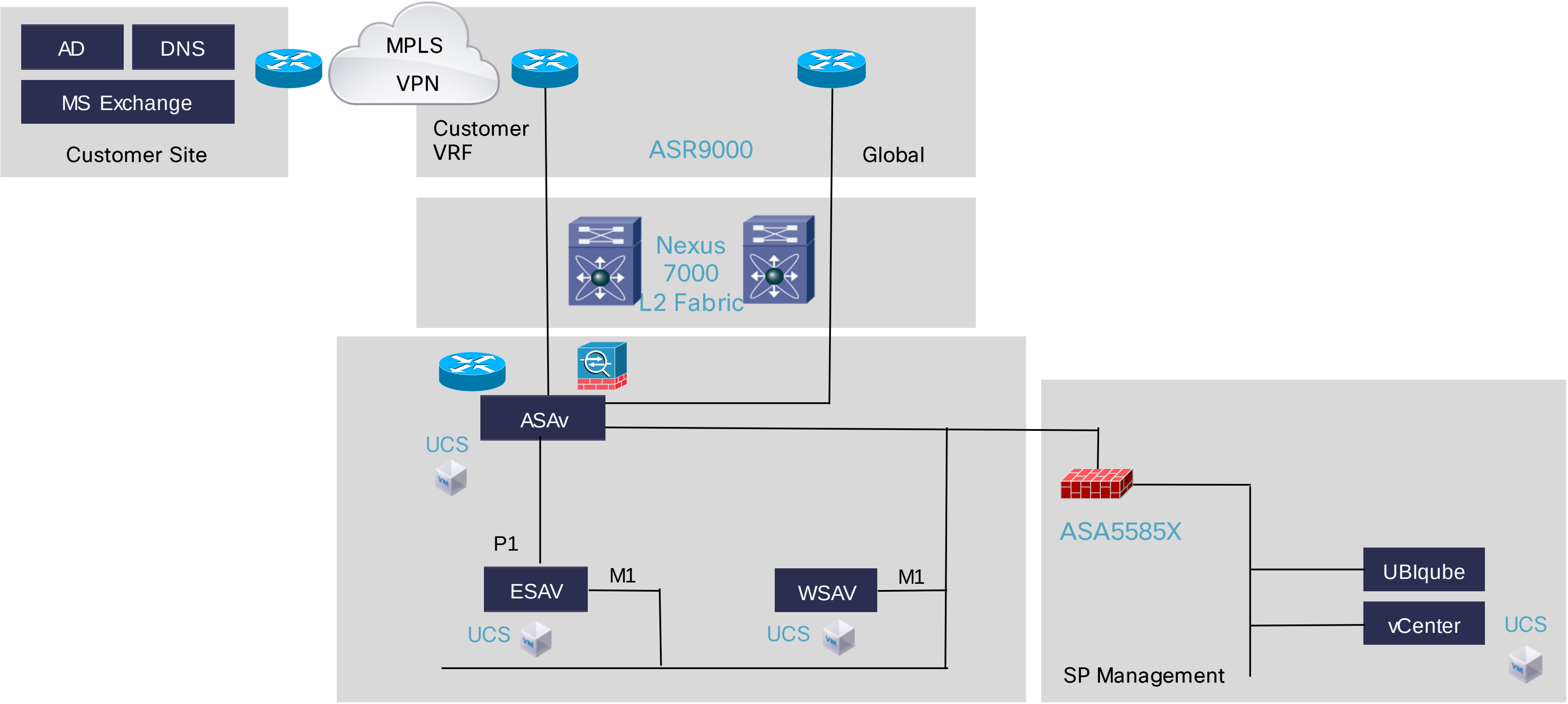
VSA 1.0 Gold Container with HSS

Use Case 1 – CSR1Kv, WSAV, ESAV



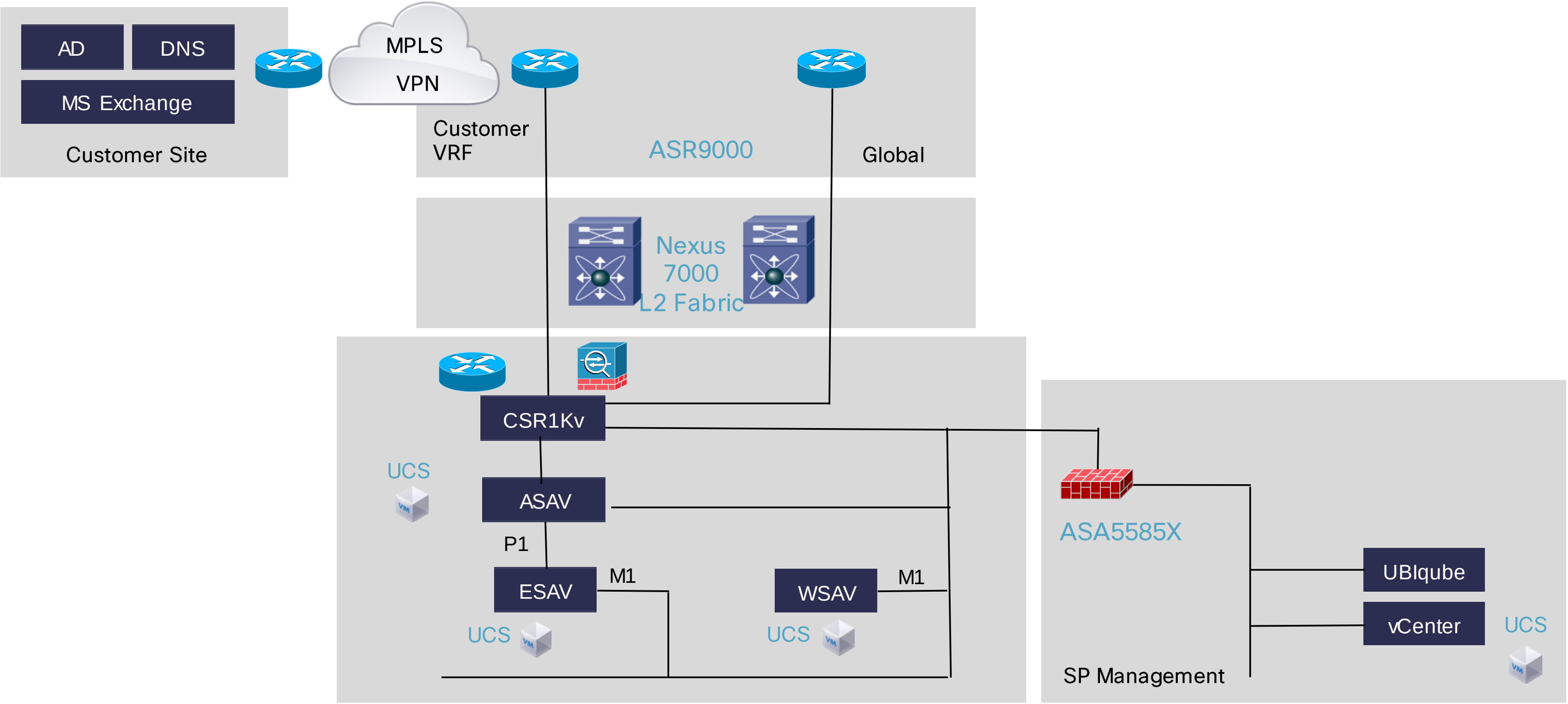
VSA 1.0 Gold Container with HSS

Use Case 2 – ASAV, WSAV, ESAV

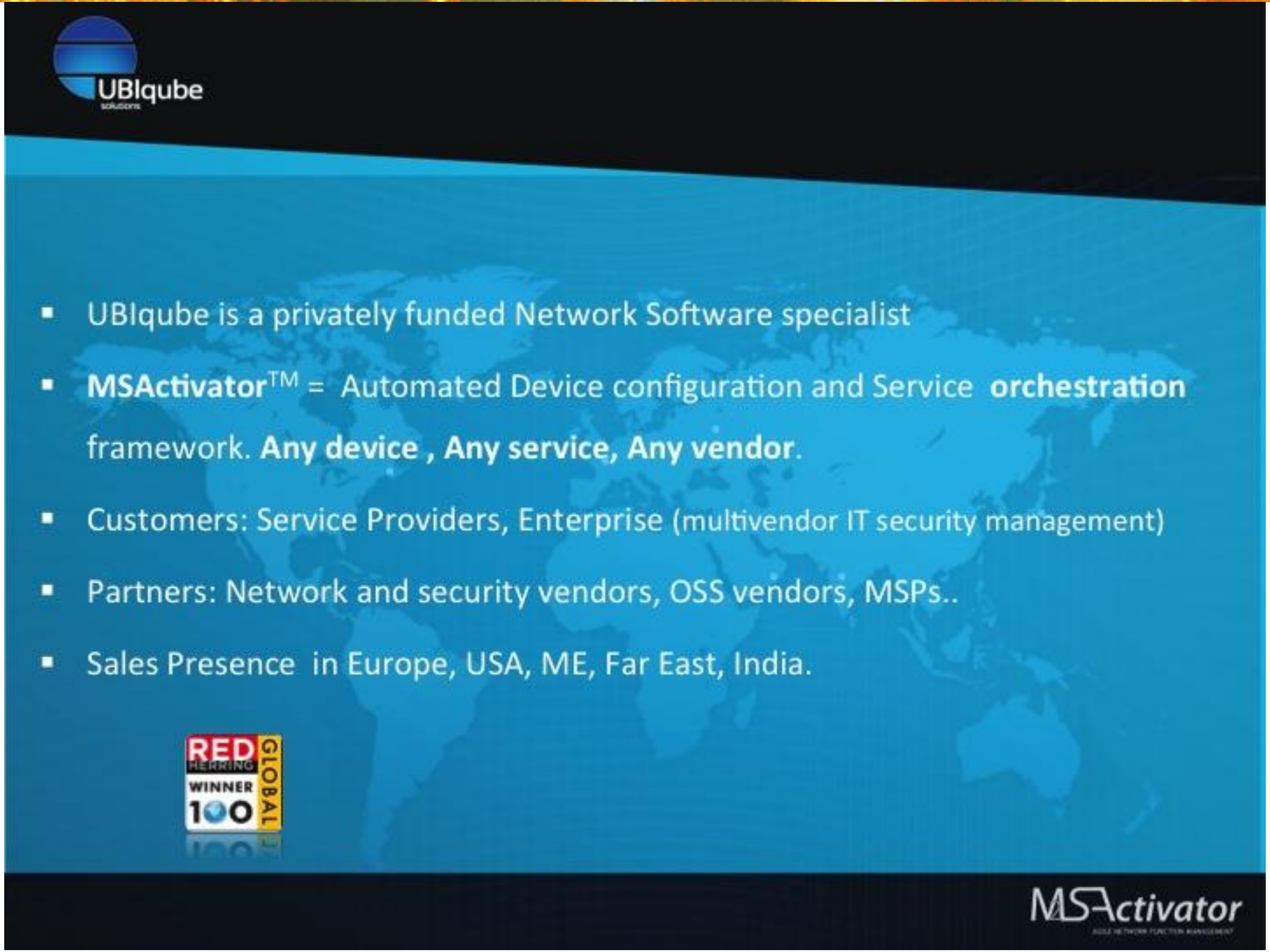


VSA 1.0 Gold Container with HSS

Use Case 3 – CSR1Kv, ASAv, WSAV, ESAV



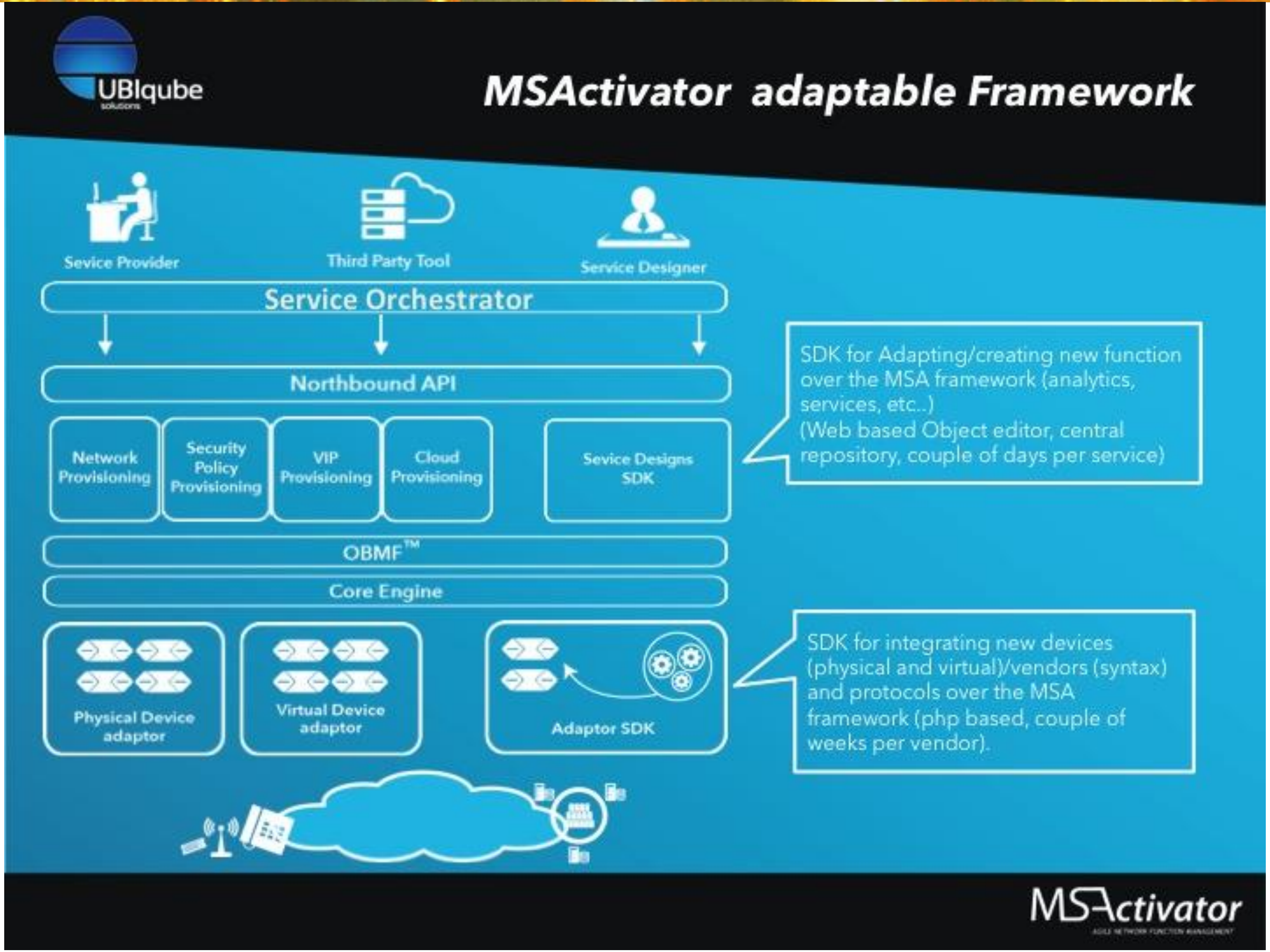
HSS Security Domain Management



UBIqube
solutions

- UBIqube is a privately funded Network Software specialist
- **MSActivator**^{TM} = Automated Device configuration and Service **orchestration** framework. **Any device , Any service, Any vendor**.
- Customers: Service Providers, Enterprise (multivendor IT security management)
- Partners: Network and security vendors, OSS vendors, MSPs..
- Sales Presence in Europe, USA, ME, Far East, India.

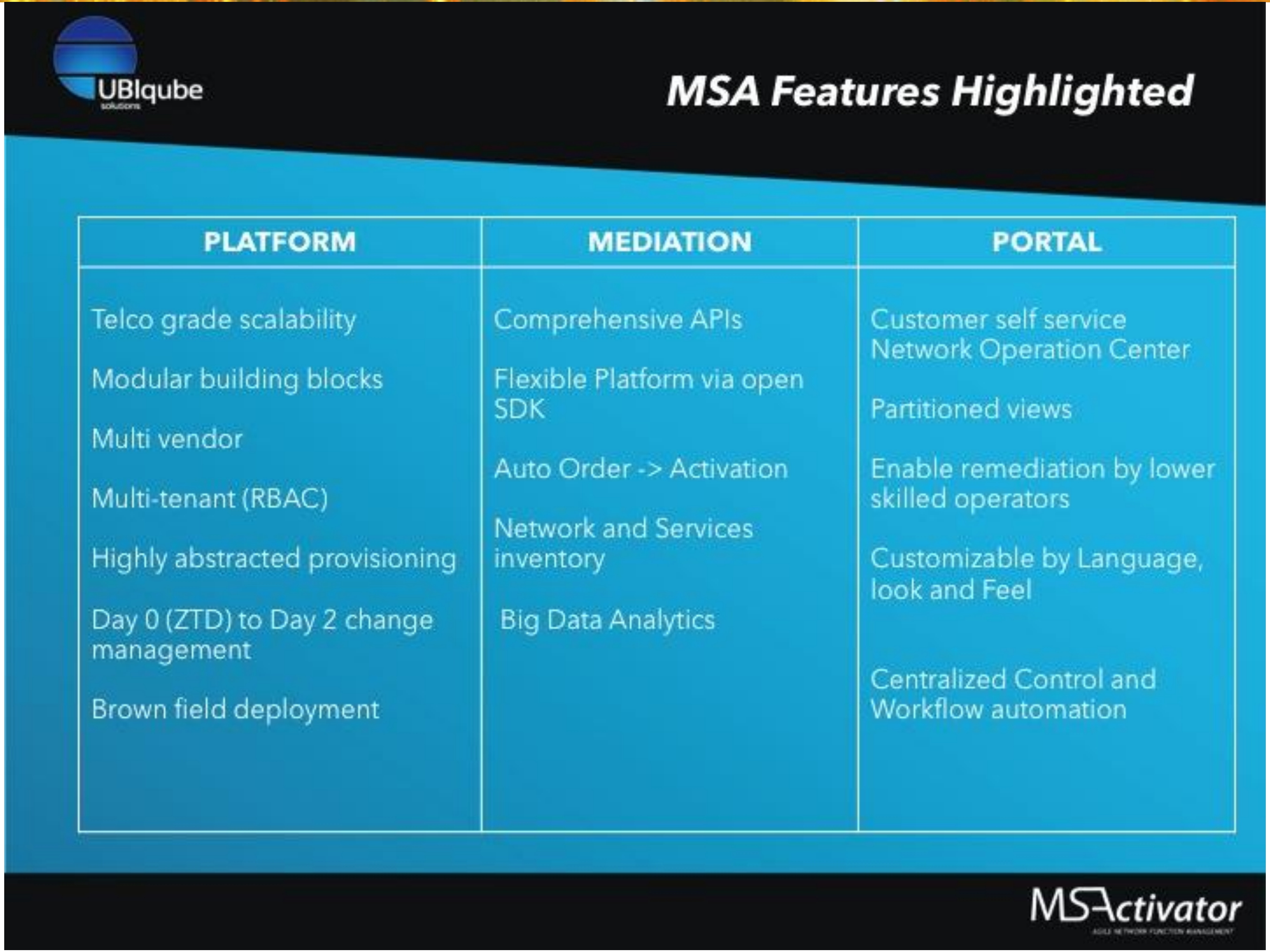
MSActivator



MSActivator adaptable Framework

SDK for Adapting/creating new function over the MSA framework (analytics, services, etc..)
(Web based Object editor, central repository, couple of days per service)

SDK for integrating new devices (physical and virtual)/vendors (syntax) and protocols over the MSA framework (php based, couple of weeks per vendor).



UBIqube

MSA Features Highlighted

PLATFORM	MEDIATION	PORTAL
Telco grade scalability Modular building blocks Multi vendor Multi-tenant (RBAC) Highly abstracted provisioning Day 0 (ZTD) to Day 2 change management Brown field deployment	Comprehensive APIs Flexible Platform via open SDK Auto Order -> Activation Network and Services inventory Big Data Analytics	Customer self service Network Operation Center Partitioned views Enable remediation by lower skilled operators Customizable by Language, look and Feel Centralized Control and Workflow automation

MSActivator

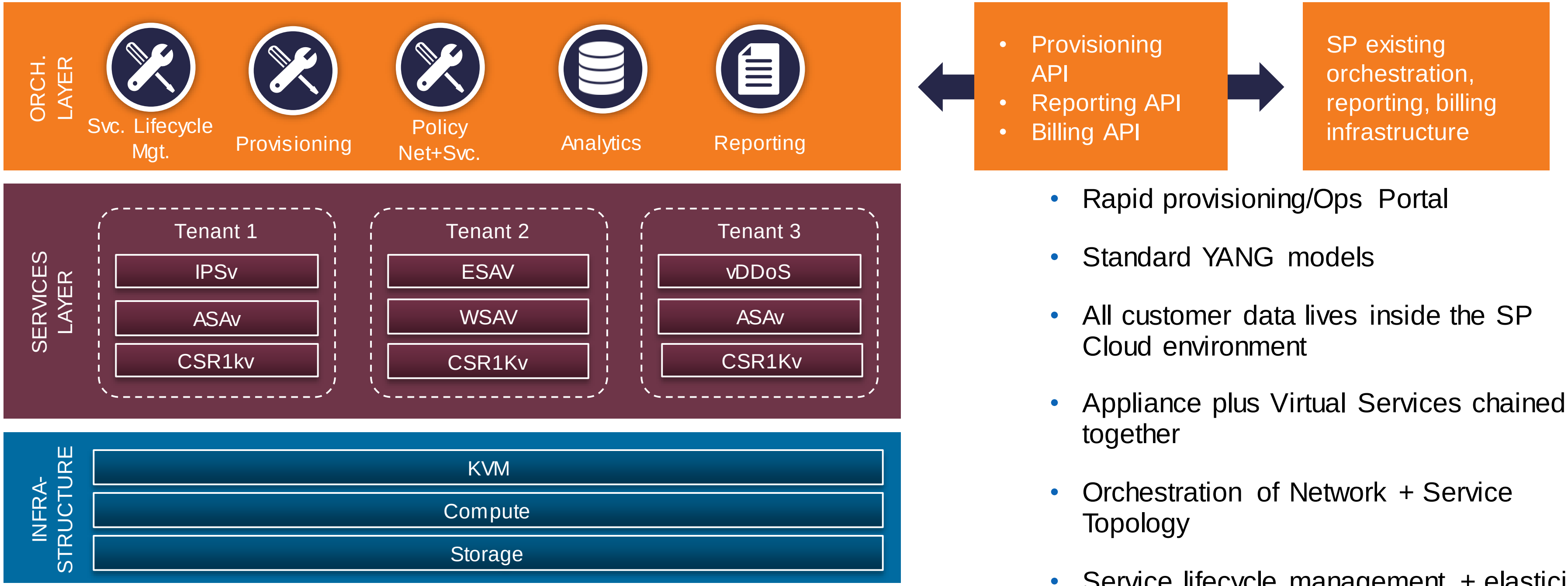
Demo: HSS

HSS References

- Hosted Security as a Service Documentation
  - www.cisco.com/go/hss
- Cisco Content Security Virtual Appliance Installation Guide
  - www.cisco.com/en/US/docs/security/content_security/virtual_appliances/Cisco_Content_Security_Virtual_Appliance_Install_Guide.pdf
- Knowledge Base and Support Tools
  - www.cisco.com/en/US/products/ps10154/tsd_products_support_series_home.html

CloudVPN

CloudVPN at a Glance



ORCH. LAYER

Svc. Lifecycle Mgt.

Provisioning

Policy Net+Svc.

Analytics

Reporting

- Provisioning API
- Reporting API
- Billing API

SP existing orchestration, reporting, billing infrastructure

SERVICES LAYER

Tenant 1

IPSv

ASAv

CSR1kv

Tenant 2

ESAV

WSAV

CSR1Kv

Tenant 3

vDDoS

ASAv

CSR1Kv

INFRA-STRUCTURE

KVM

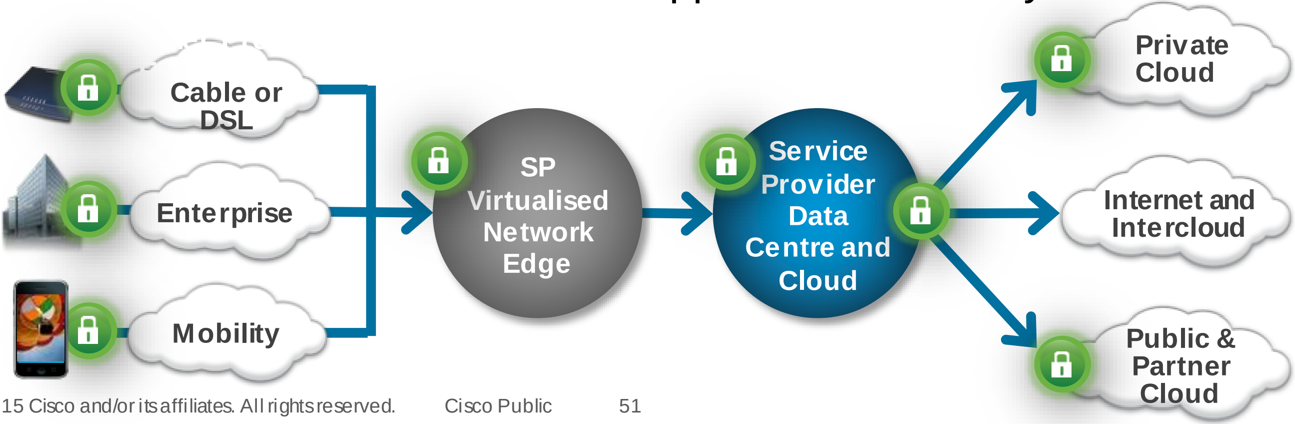
Compute

Storage

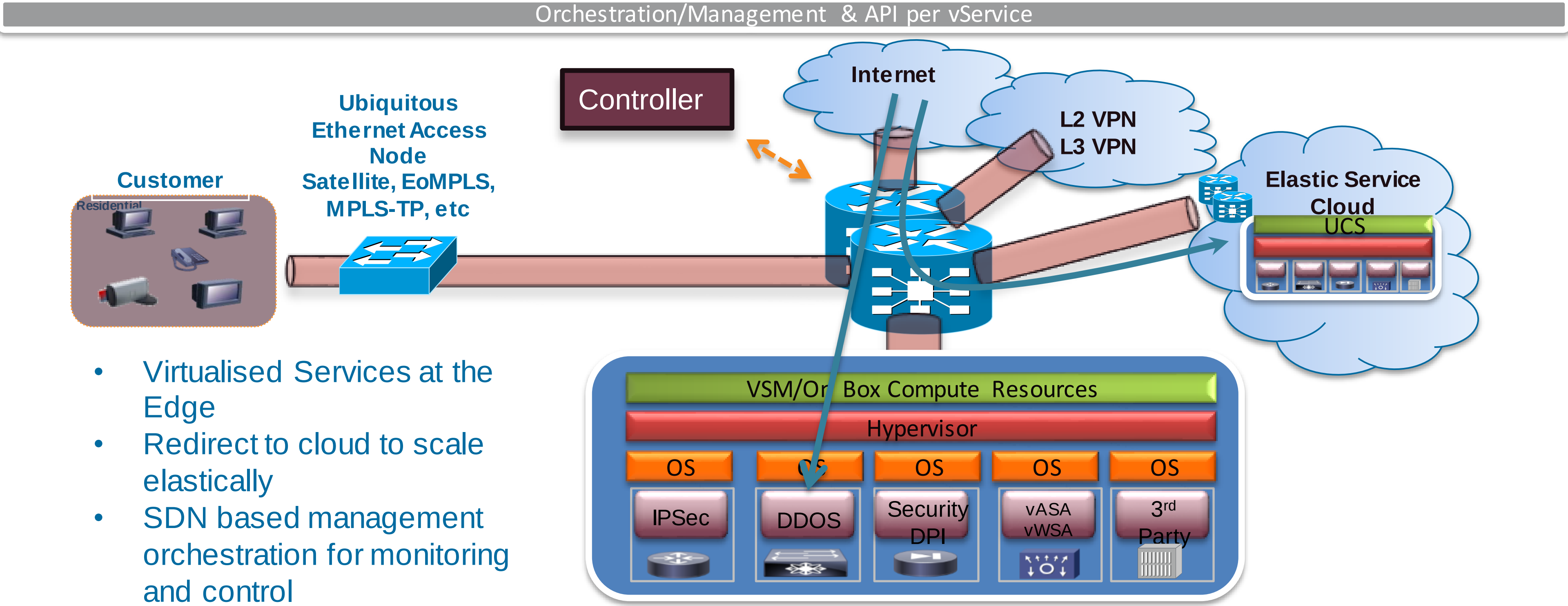
- Rapid provisioning/Ops Portal
- Standard YANG models
- All customer data lives inside the SP Cloud environment
- Appliance plus Virtual Services chained together
- Orchestration of Network + Service Topology
- Service lifecycle management + elasticity + workload placement
- IPv6 deployed here

Hosted Security as a Service

- Security is all about two concepts: Visibility & Control
- Threats are mitigated as close to the source as possible
- Security services are dynamically chained together and instantiated to form a service chain to mitigate a specific threat and/or to provide a managed security service on distributed compute resources
- Threat defence provides a distributed capability to mitigate threats – targeted at the network, the Data Centre, the Cloud and the applications that they serve



Elastic Security Services – Places in the Network

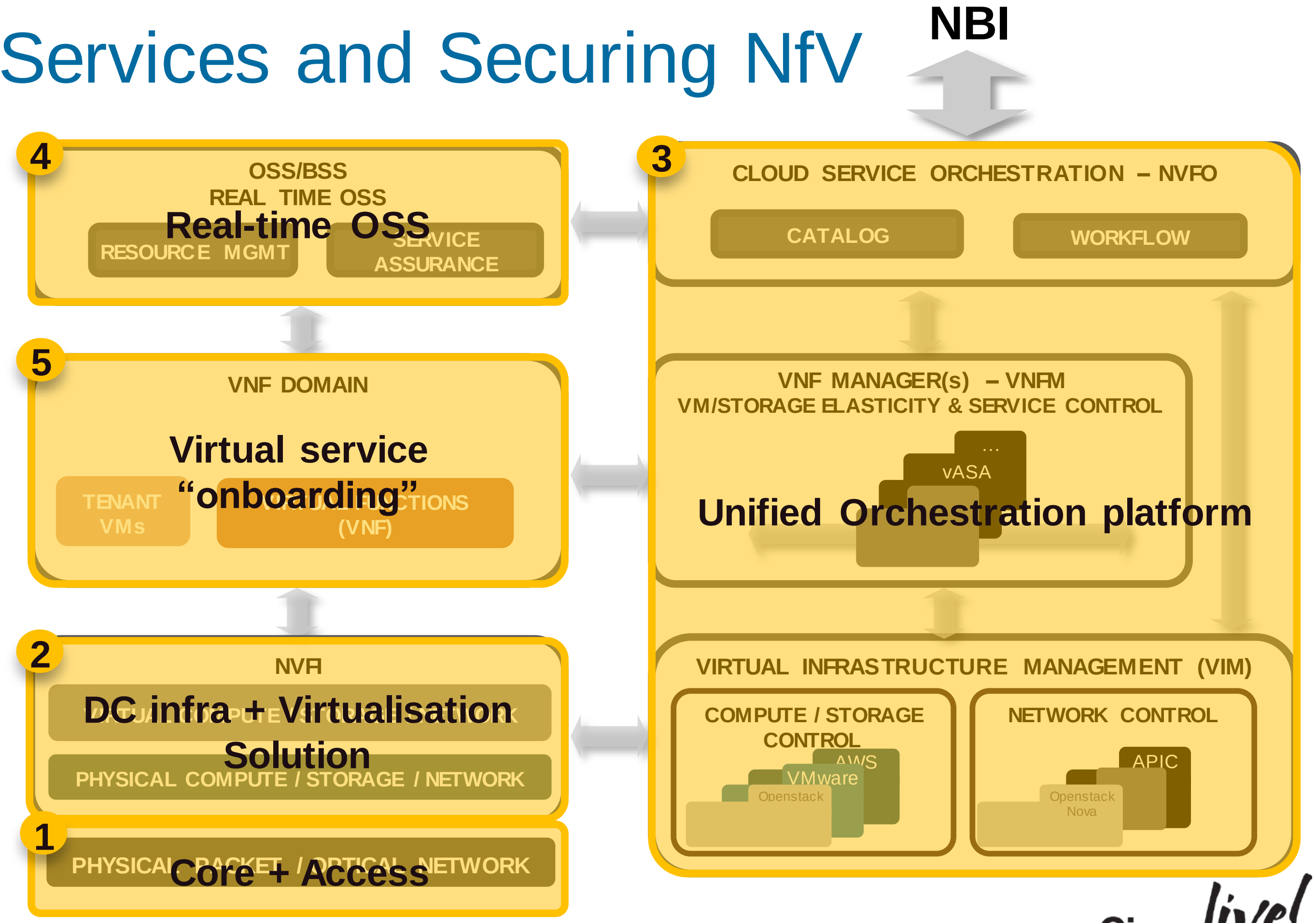

Orchestration/Management & API per vService
Controller
Internet
L2 VPN
L3 VPN
Elastic Service Cloud
UCS
Customer
Residential
Ubiquitous Ethernet Access Node
Satellite, EoMPLS, MPLS-TP, etc
VSM/On Box Compute Resources
Hypervisor
OS
OS
OS
OS
OS
IPSec
DDOS
Security DPI
vASA
vWSA
3rd Party

- Virtualised Services at the Edge
- Redirect to cloud to scale elastically
- SDN based management orchestration for monitoring and control

Same virtual services on the edge and in the cloud, managed through a common central monitoring and orchestration system

NfV Security Services and Securing NfV

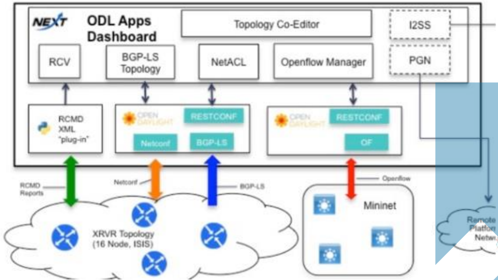
- Components:
  - Evolved IP+Optical network architecture
  - DC infra + virtualisation
  - Unified orchestration platform – Openstack focussed
  - Real-time OSS
  - Virtual service "on-boarding"


NBI
4
OSS/BSS
REAL TIME OSS
Real-time OSS
RESOURCE MGMT
SERVICE ASSURANCE
5
VNF DOMAIN
Virtual service "onboarding"
TENANT VMs
VIRTUAL FUNCTIONS (VNF)
2
NVFI
DC infra + Virtualisation Solution
VIRTUAL COMPUTE / STORAGE / NETWORK
PHYSICAL COMPUTE / STORAGE / NETWORK
1
PHYSICAL PACKET / OPTICAL NETWORK
Core + Access
3
CLOUD SERVICE ORCHESTRATION – NVFO
CATALOG
WORKFLOW
VNF MANAGER(s) – VNFM
VM/STORAGE ELASTICITY & SERVICE CONTROL
...
vASA
Unified Orchestration platform
VIRTUAL INFRASTRUCTURE MANAGEMENT (VIM)
COMPUTE / STORAGE CONTROL
AWS
VMware
Openstack
NETWORK CONTROL
APIC
Openstack Nova

How To Dynamically Build and Test Services

The Innovation Pod Program

ODL

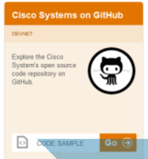


DevNet Map

DEVNET

Try this easy-to-use, dynamic navigation tool for exploring Cisco DevNet. Simply click to expand the map and locate the pages you need in seconds.

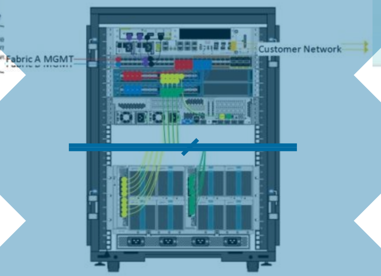
TOOL Go


Cisco Systems on GitHub

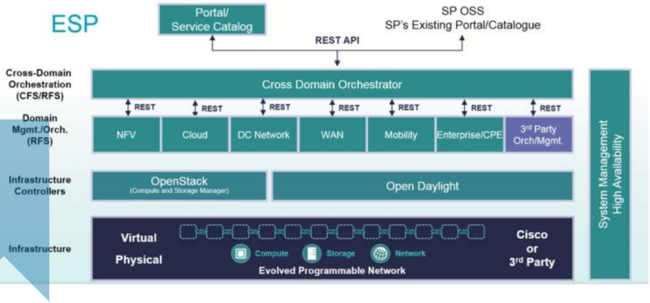
DEVNET

Explore the Cisco System's open source code repository on GitHub.

CODE SAMPLE Go



ESP



SDN and Virtualization Portfolio

Mobile Packet Core
EPC (QvPC SSI)
PCRF
Video/Home Services
CDN Content Acquisition
CDN Policy Control
CDN Analytics
Video Service Router
Core/Metro
vRouteReflector (IOS XRv)
Cloud/DC
SDN Controller (XNC)
vSwitch (Nexus 1Kv)
Managed Services
Virtual Services (12)*
vCPE, FW, IPSec/SSL,
WLAN, etc.

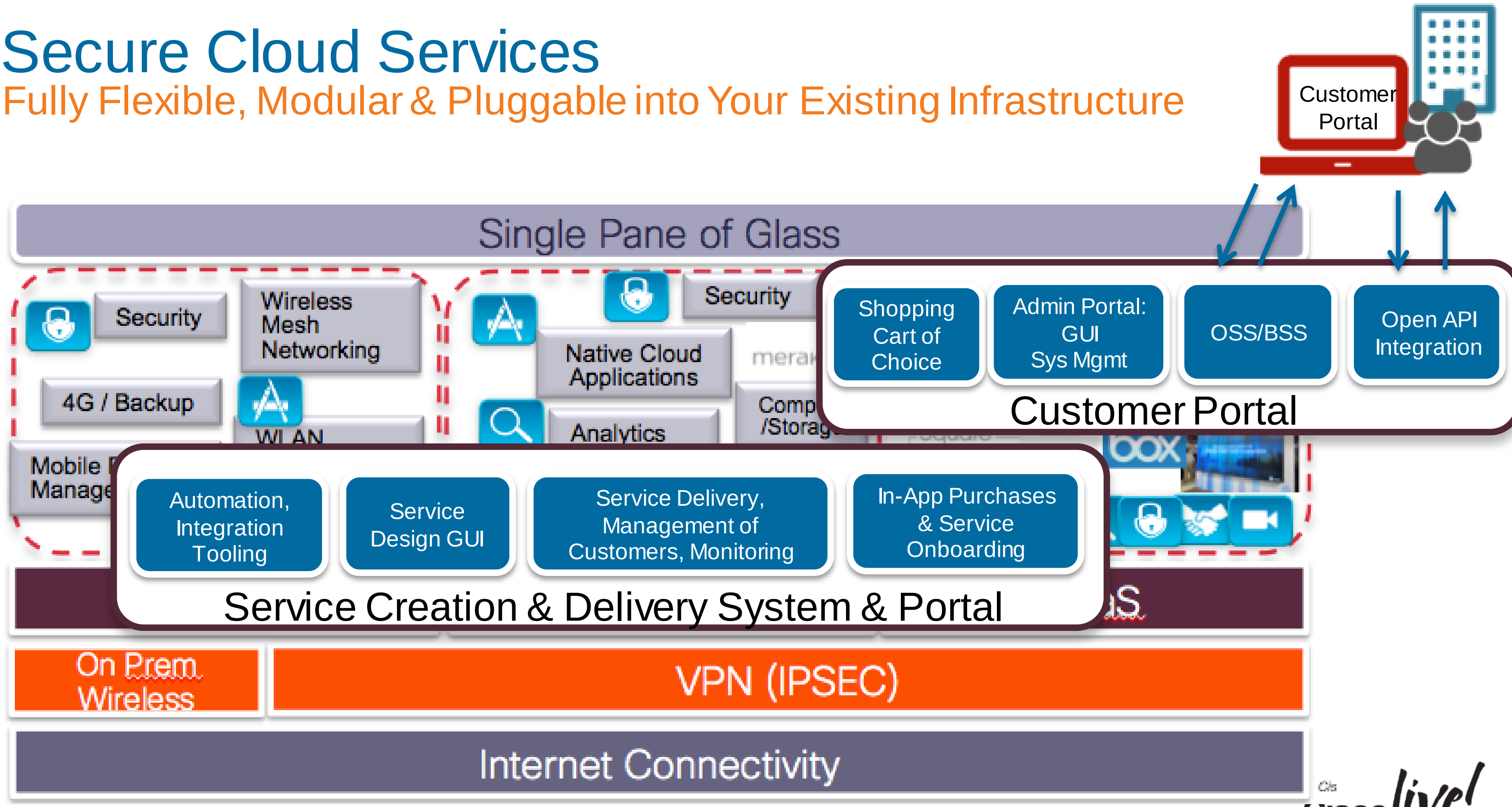
Mobility Packet Core
MOG
Video/Home Services
Cloud DVR
Core/Metro
SDN Controller (QWAVE)
Cloud/DC
Orchestration Platform (ESP)
OpenStack
High Performance L3 vFwd
Elasticity & Svc Chaining
Managed Services
SDN Controller - CPE

Mobile Packet Core
EPC (QvPC SCALE)
Gi-LAN Services
SECGW
SGGN/MME
QSON
SaMOG-TWAP/G
Video/Home Services
Elastic CDN
Core/Metro
TE Mgr App for QWAVE
Cloud/DC
Orchestration Platform (ESP)

Core/Metro
Virtual (Provider) Edge Router
QWAVE L1-L3 Convergence

Secure Cloud Services

Fully Flexible, Modular & Pluggable into Your Existing Infrastructure



Customer Portal

Single Pane of Glass

Security

Wireless Mesh Networking

4G / Backup

WLAN

Mobile D Manage

Security

Native Cloud Applications

merak

Analytics

Comp /Storag

box

Shopping Cart of Choice

Admin Portal: GUI Sys Mgmt

OSS/BSS

Open API Integration

Customer Portal

Automation, Integration Tooling

Service Design GUI

Service Delivery, Management of Customers, Monitoring

In-App Purchases & Service Onboarding

Service Creation & Delivery System & Portal

aS

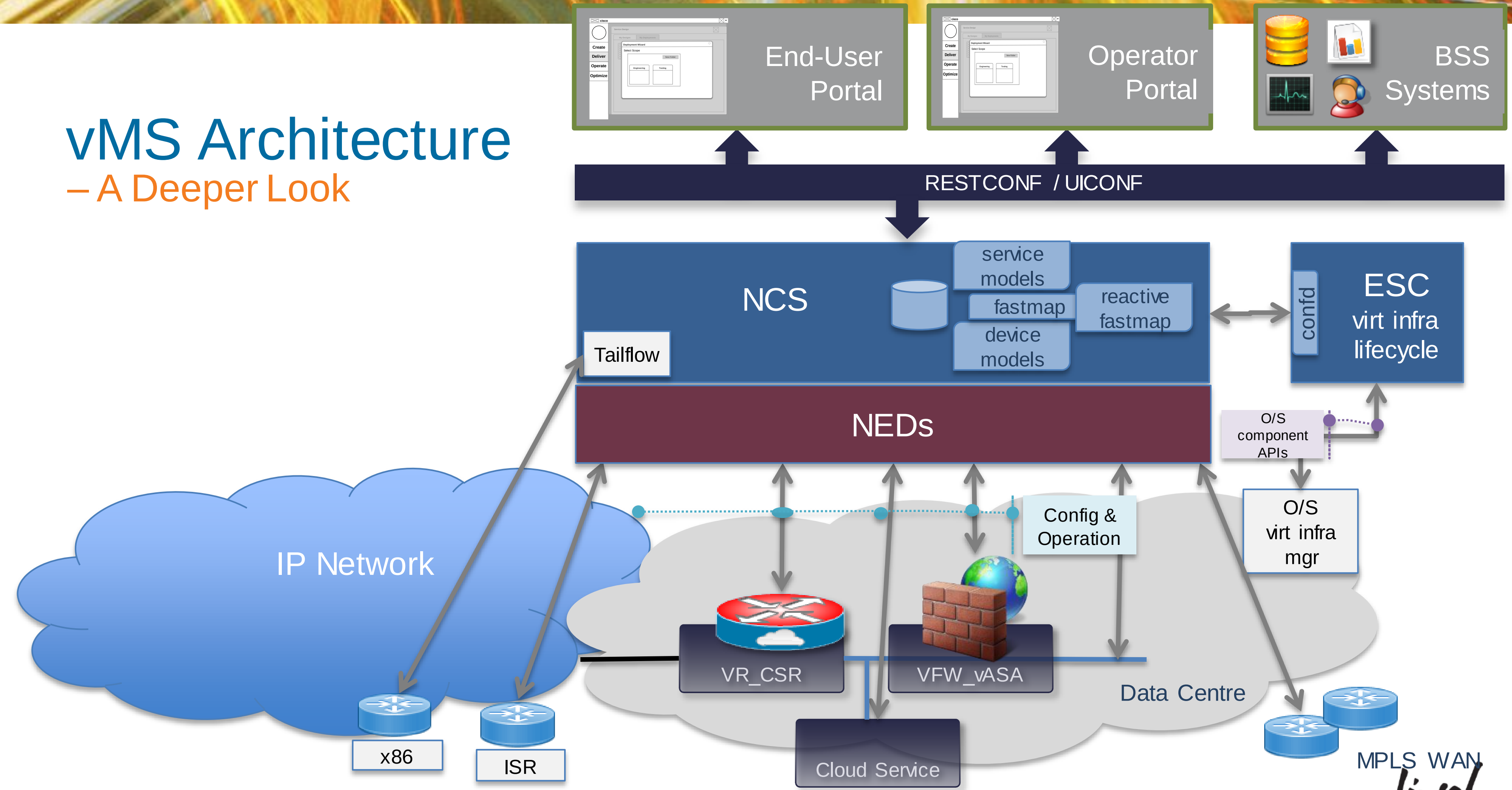
On Prem Wireless

VPN (IPSEC)

Internet Connectivity

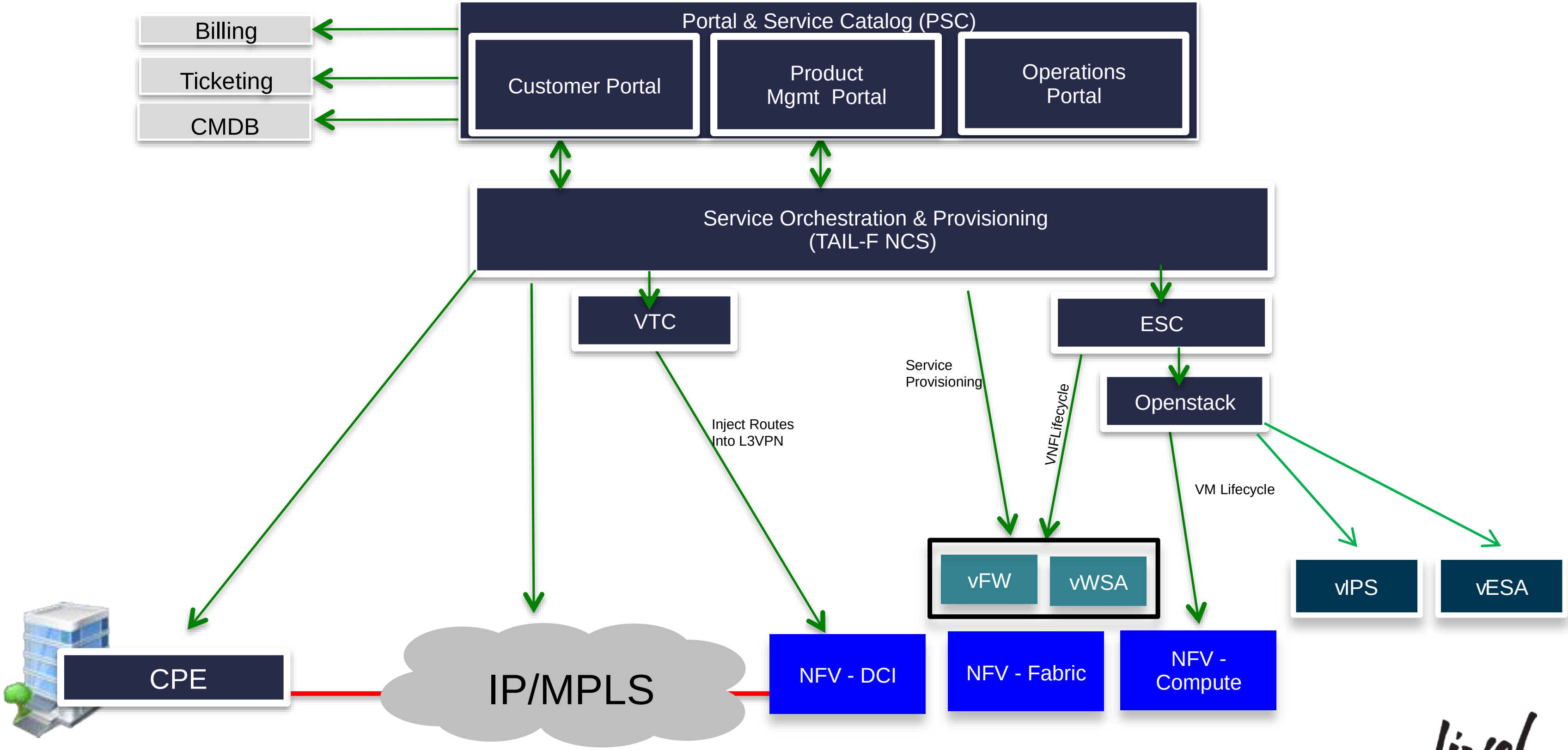
vMS Architecture

– A Deeper Look



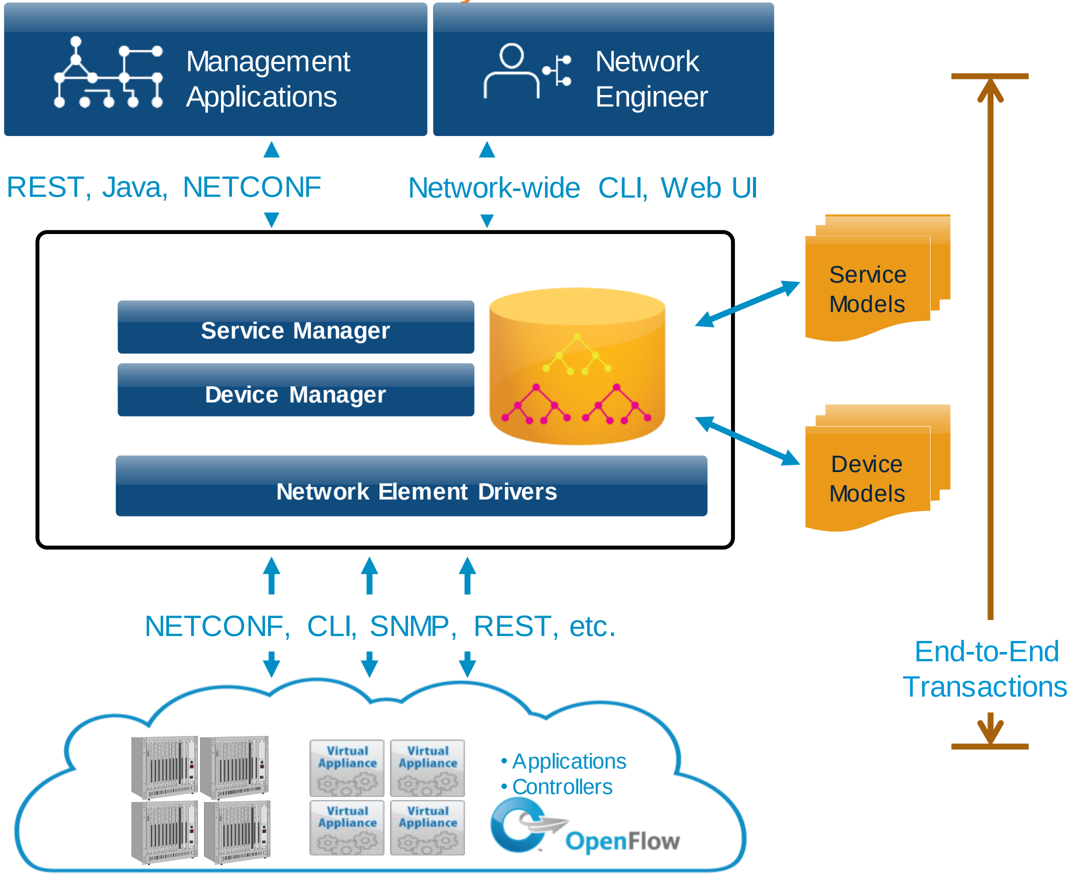
vMS

– A deeper view



Centre of vMS Orchestration

Tail-f Network Control System Overview



Multi-vendor service orchestrator for existing and future networks

Single pane of glass for:

- L2-L7 networking
- Hardware Devices
- Virtual Appliances
- OpenFlow Switches

Tail-F Network Control System provides abstractions based on

- Data models
- Transactions

Sold to service providers

Perpetual license

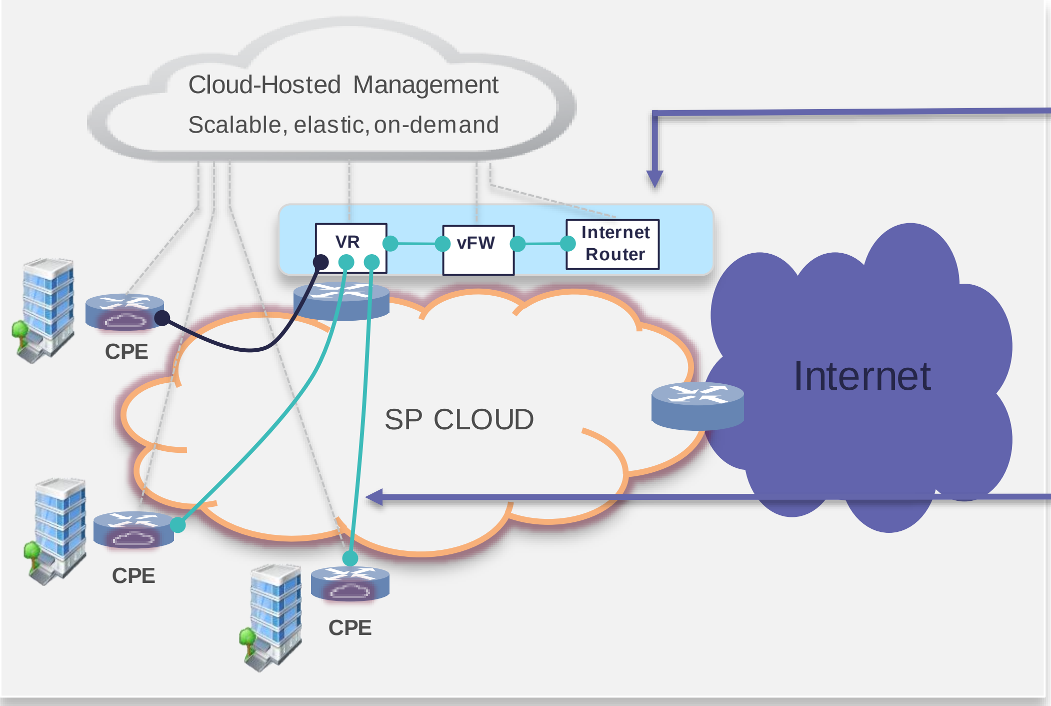
vMS Service Bundles

- **(1) Internet Access (IA)**, **FWaaS**, **VPNaaS**
  - CSR1kv, vASA with NAT, FW, RA.
- **(2) IA**, **FWaaS**, **VPNaaS** and **WSaaS**
  - CSR1kv, vASA, vWSA
- **(3) IA**, **FWaaS**, **VPNaaS** and **Next-Gen IPSaaS**
  - CSR1kv, vASA, vWSA, vNG-IPS(SourceFire)
- **4) IA**, **FWaaS**, **VPNaaS** and **IdentityaaS**
  - CSR1kv, vASA, vISE with NAT, BYOD, Policy, TrustSec
- **(5) IA**, **FWaaS**, **VPNaaS** and **ESaaS**
  - CSR1kv, vASA, vESA
- **(6) IA**, **FWaaS**, **VPNaaS** and **DDoSaaS**

Flexibility for other variations based on marketing needs

CloudVPN Business Services:

Use Case 1: CloudVPN with Internet, Firewall (FW), Remote Access (RA)



Cloud IPVPN with FW and Remote Access to Internet

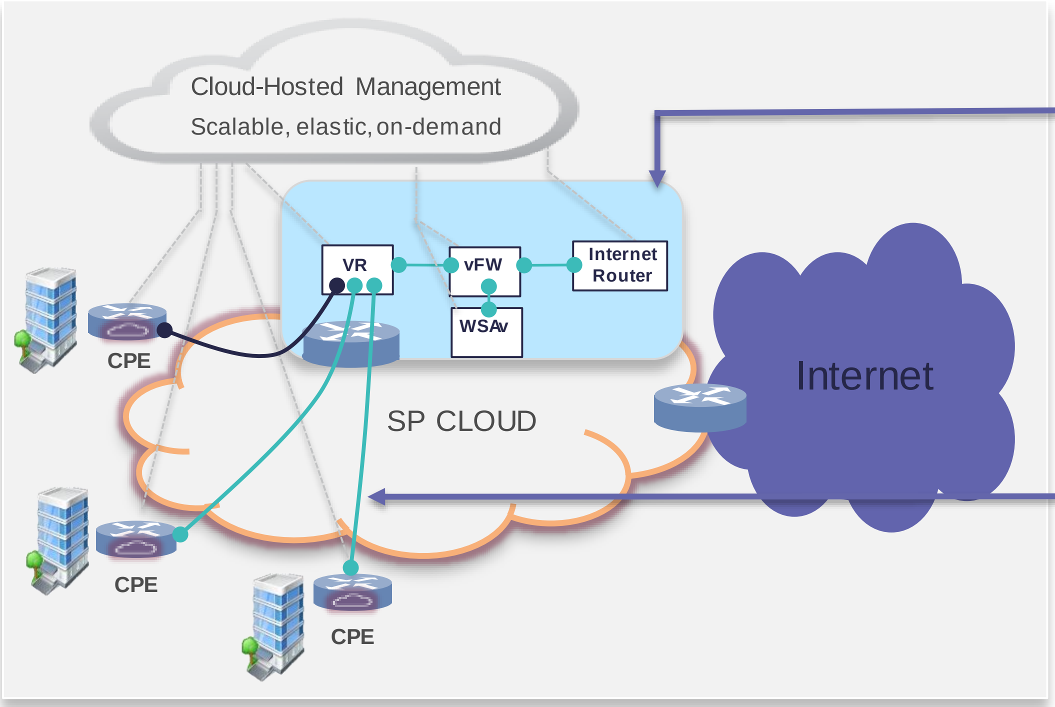
- vFW with NAT and Policy
- vFW with IPSec/SSL Remote Access including Remote End-Host posture verification

Overlay Packet Tunnels

- Keyed IPv6 tunnels - mesh, hub&spoke;
- IPSec tunnels – mesh, hub&spoke if keyed IPv6 tunnels not supported;

CloudVPN Business Services:

Use Case 2: CloudVPN with Internet, FW, RA and Enhanced Web Security



Cloud IPVPN with FW and Remote Access to Internet

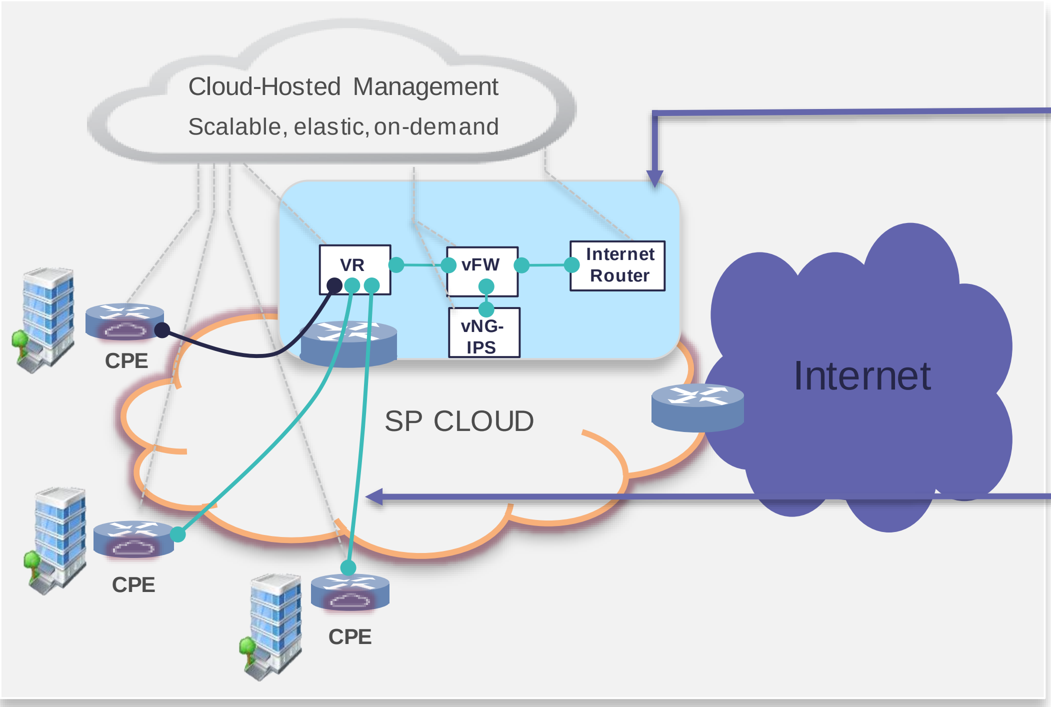
- vFW with NAT and Policy
- vFW with IPSec/SSL Remote Access including Remote End-Host posture verification
- WSAv for Enhanced Web Security

Overlay Packet Tunnels

- Keyed IPv6 tunnels - mesh, hub&spoke;
- IPSec tunnels – mesh, hub&spoke if keyed IPv6 tunnels not supported;

CloudVPN Business Services:

Use Case 3: CloudVPN with Internet, FW, RA and Next-Gen-IPS



Cloud IPVPN with FW and Remote Access to Internet

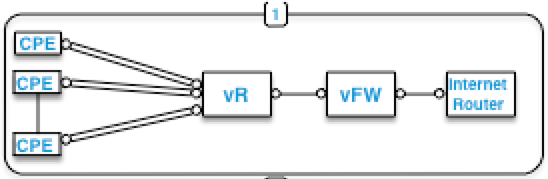
- vFW with NAT and Policy
- vFW with IPSec/SSL Remote Access including Remote End-Host posture verification
- vNG-IPS (SourceFire) for advanced threat protection and real-time contextual awareness

Overlay Packet Tunnels

- Keyed IPv6 tunnels - mesh, hub&spoke;
- IPSec tunnels – mesh, hub&spoke if keyed IPv6 tunnels not supported;

Virtual Security Workflows

Reference Slide

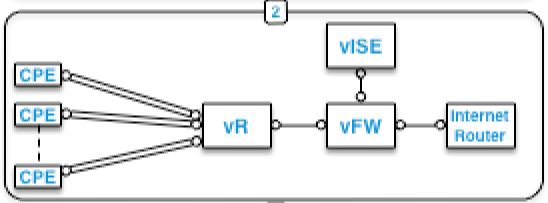


1

vIPVPN with FW and RA

-vFW with NAT and FW policy.

-vFW with IPSec/SSL Remote Access (RA) incl. remote end-host security posture verification.



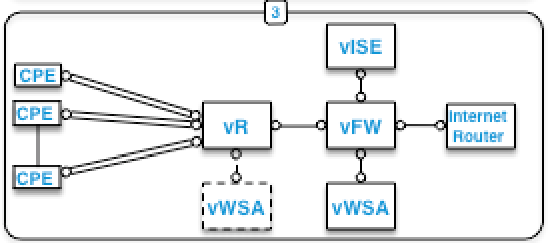
2

vIPVPN with BYOD, FW and RA

-vFW with NAT and FW policy.

-vFW with IPSec/SSL remote access incl. remote end-host security posture verification.

-vISE for BYOD svc auth (AAA, trust-sec label to IP binding)



3

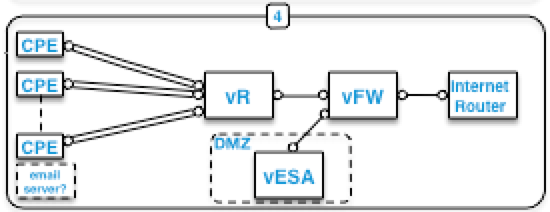
vIPVPN with BYOD, FW, RA, WebSec

-vFW with NAT and FW policy.

-vFW with IPSec/SSL remote access incl. remote end-host security posture verification.

-vISE for BYOD svc auth (AAA, trust-sec label to IP binding)

- vWSA for Enhanced Web Security



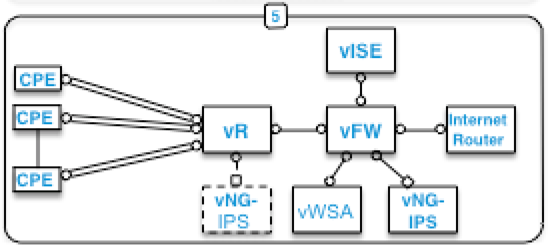
4

vIPVPN with BYOD, FW, RA, EmailSec

-vFW with NAT and FW policy.

-vFW with IPSec/SSL remote access incl. remote end-host security posture verification.

-vESA for Critical Information Protection (inbound and outbound Emails)



5

vIPVPN with BYOD, FW, RA, WebSec, ngIPS

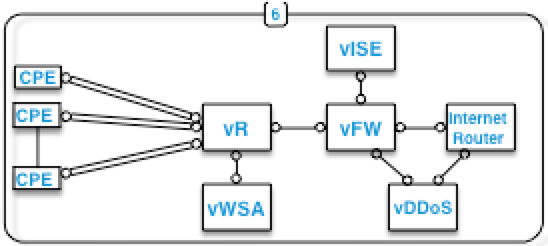
-vFW with NAT and FW policy.

-vFW with IPSec/SSL remote access incl. remote end-host security posture verification.

-vISE for BYOD svc auth (AAA, trust-sec label to IP binding)

- vWSA for Enhanced Web Security

-vNG-IPS (SourceFire) for advanced threat protection and real-time contextual awareness



6

vIPVPN with BYOD, FW, RA, WebSec, DDoS

-vFW with NAT and FW policy.

-vFW with IPSec/SSL remote access incl. remote end-host security posture verification.

-vISE for BYOD svc auth (AAA, trust-sec label to IP binding)

- vWSA for Enhanced Web Security

-vDDoS (Radware DefensePro) for volumetric and application DDoS visibility and mitigation services

Packet links

═ tunnel

— local link

Termination points

═○ —○ L3

═□ —□ L2

Packet service nodes

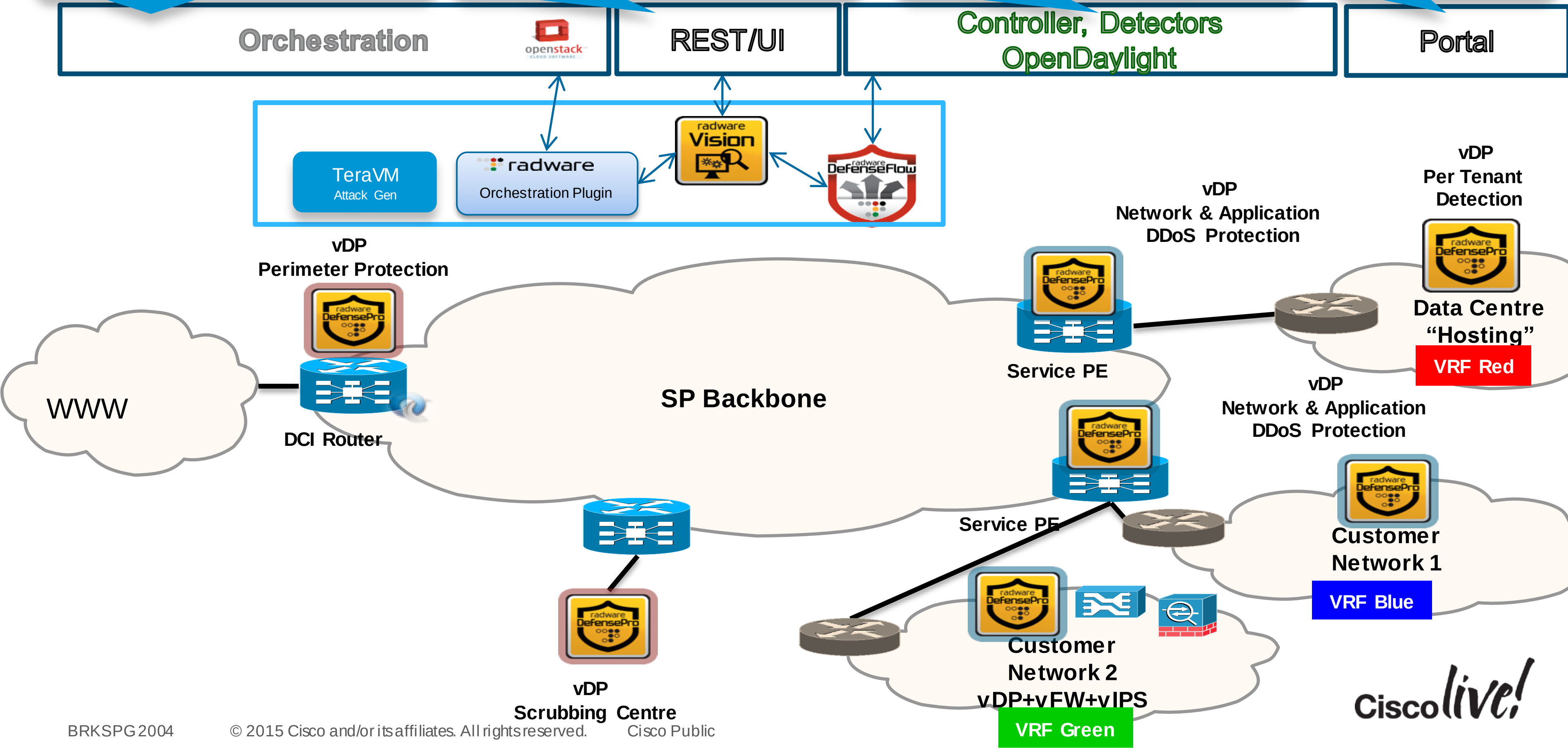
vR	router	vWSA	web security appliance
vLB	load balancer	vESA	email security appliance
Internet Router	Internet Router	vISE	identity services engine
L3vpn	L3 vpn	vFW	fire wall
L2vpn	L2 vpn	vNG-IPS	intrusion protection system
L3net	L3 network	vDDoS	ddos mitigation services
L2net	L2 network		

Brings up Compute and Storage
Installer is used

Used for provisioning of the chain service, Interface for automation & for OSS system

Open Daylight
Receives attack information out of the network, reprograms the network and DefencePro App to
Mitigate automatically

Admin to book the service, triggers the Spin up of the chain



Orchestration

openstack

REST/UI

Controller, Detectors
OpenDaylight

Portal

TeraVM
Attack Gen

radware
Orchestration Plugin

radware
Vision

radware
DefenseFlow

vDP
Perimeter Protection

DCI Router

WWW

SP Backbone

vDP
Network & Application
DDoS Protection

Service PE

vDP
Per Tenant
Detection

Data Centre
“Hosting”

VRF Red

vDP
Network & Application
DDoS Protection

Service PE

Customer
Network 1

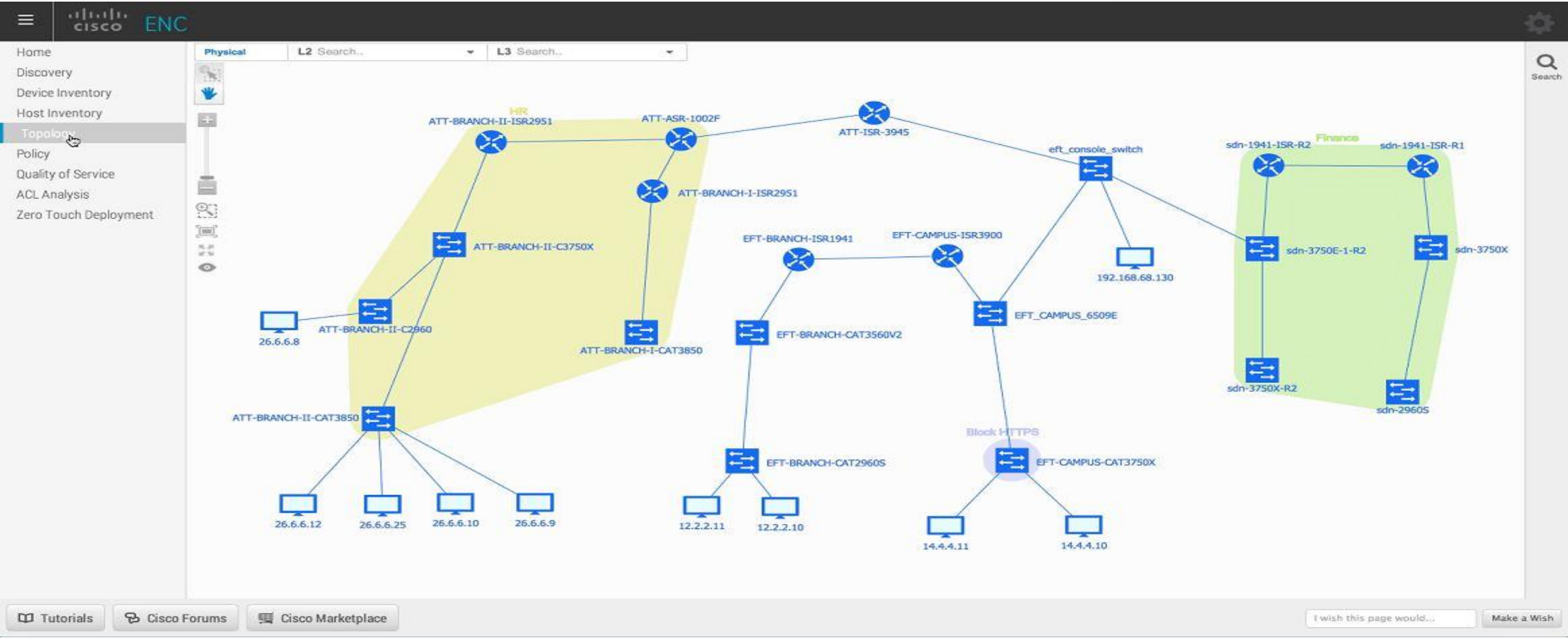
VRF Blue

Customer
Network 2
vDP+vFW+vIPS

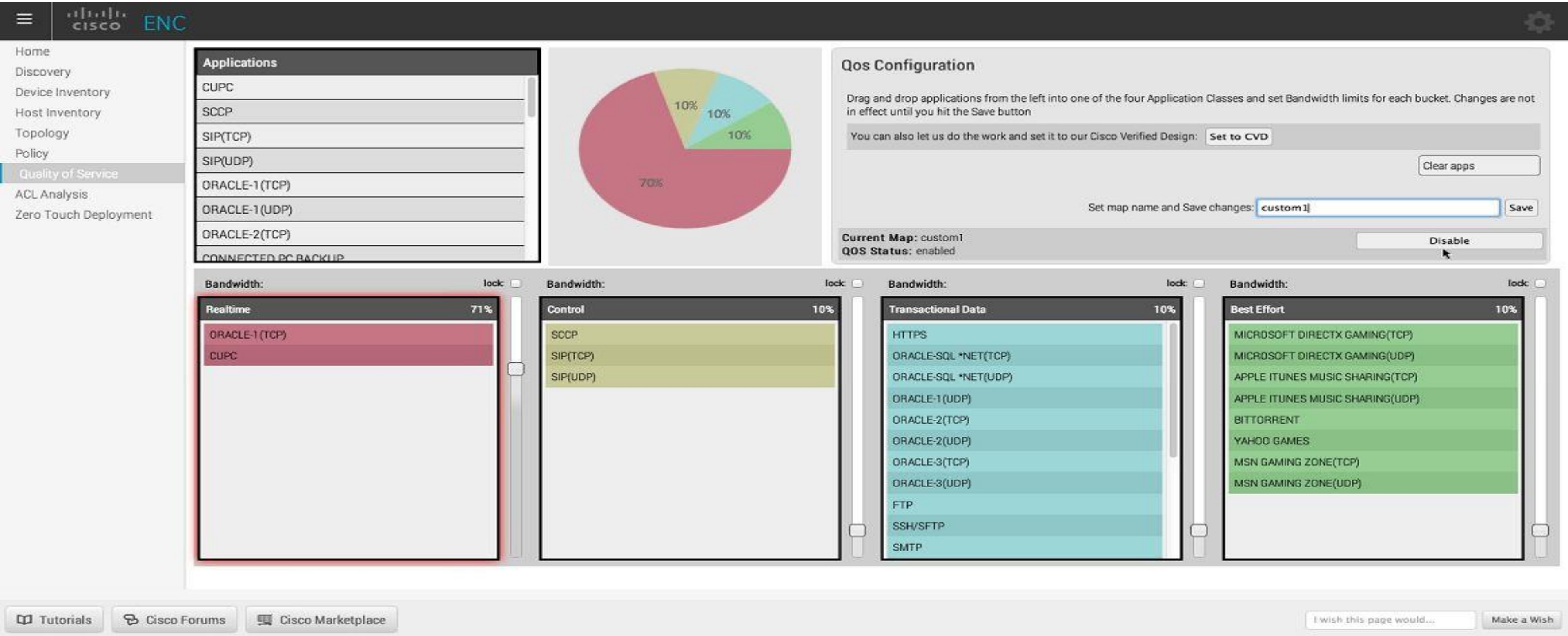
VRF Green

vDP
Scrubbing Centre

SDN Controller Visibility Application



SDN Controller: QoS Management Application



Applications

- CUPC
- SCCP
- SIP(TCP)
- SIP(UDP)
- ORACLE-1(TCP)
- ORACLE-1(UDP)
- ORACLE-2(TCP)
- CONNECTED PC BACKUP

Qos Configuration

Drag and drop applications from the left into one of the four Application Classes and set Bandwidth limits for each bucket. Changes are not in effect until you hit the Save button

You can also let us do the work and set it to our Cisco Verified Design: Set to CVD

Clear apps

Set map name and Save changes: custom1 Save

Current Map: custom1
QOS Status: enabled

Disable

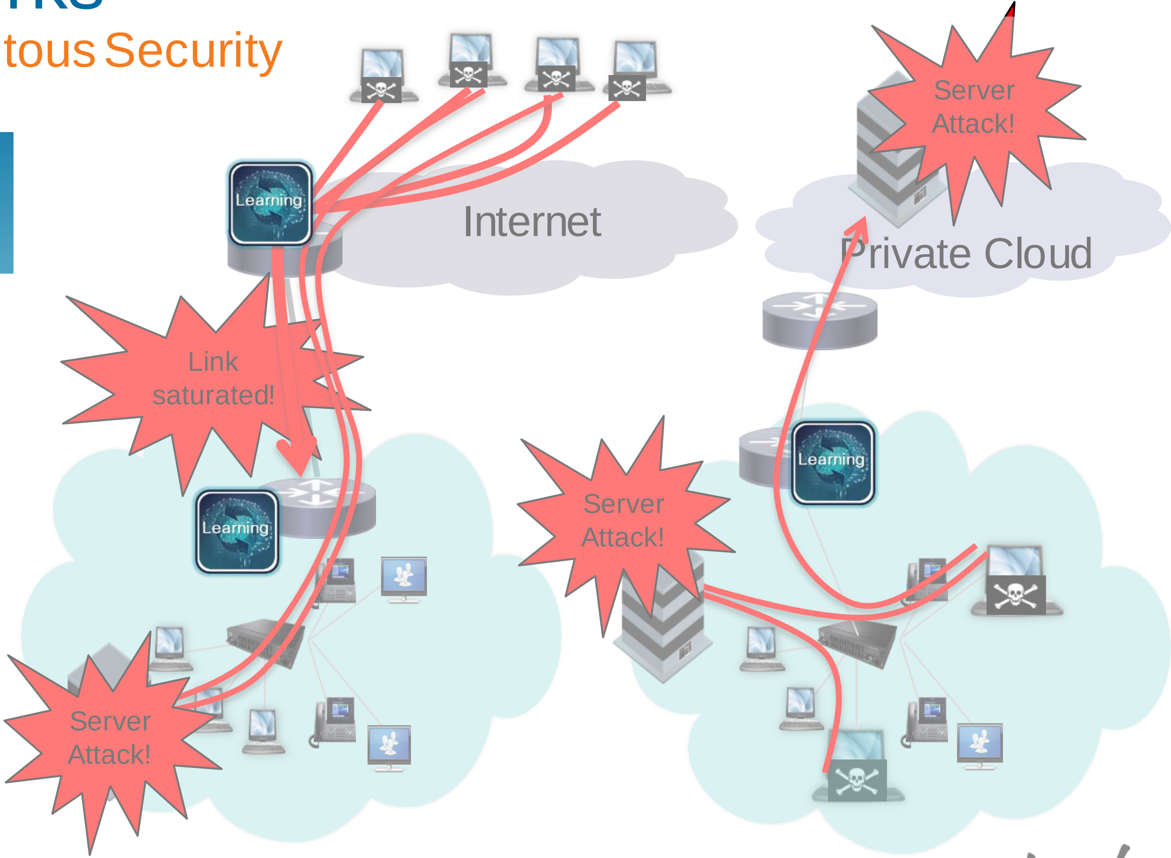
Bandwidth: lock: □	Bandwidth: lock: □	Bandwidth: lock: □	Bandwidth: lock: □
Realtime 71%	**Control 10%**	**Transactional Data 10%**	**Best Effort 10%**
ORACLE-1(TCP)	SCCP	HTTPS	MICROSOFT DIRECTX GAMING(TCP)
CUPC	SIP(TCP)	ORACLE-SQL *NET(TCP)	MICROSOFT DIRECTX GAMING(UDP)
	SIP(UDP)	ORACLE-SQL *NET(UDP)	APPLE ITUNES MUSIC SHARING(TCP)
		ORACLE-1(UDP)	APPLE ITUNES MUSIC SHARING(UDP)
		ORACLE-2(TCP)	BITTORRENT
		ORACLE-2(UDP)	YAHOO GAMES
		ORACLE-3(TCP)	MSN GAMING ZONE(TCP)
		ORACLE-3(UDP)	MSN GAMING ZONE(UDP)
		FTP	
		SSH/SFTP	
		SMTP	

Self Learning Networks

Network as a Sensor for Ubiquitous Security

Distributed Analytics for Security

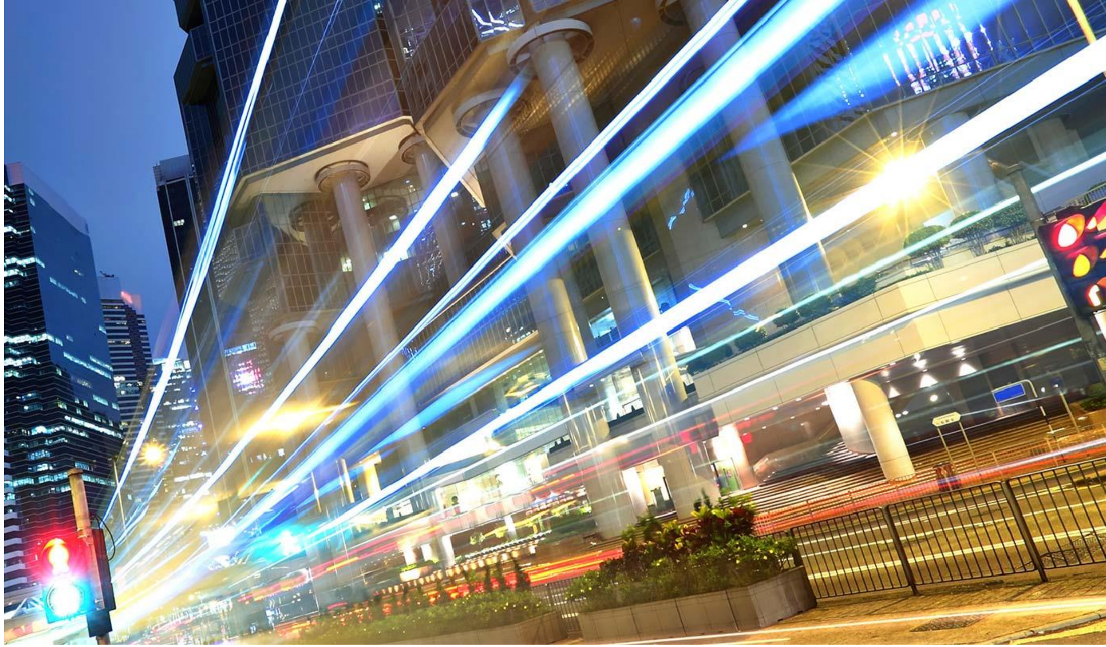
- DoS attacks get extremely hard to combat ("Subtle" and highly impactful)
- Highly Distributed
- From the Internet and within the network



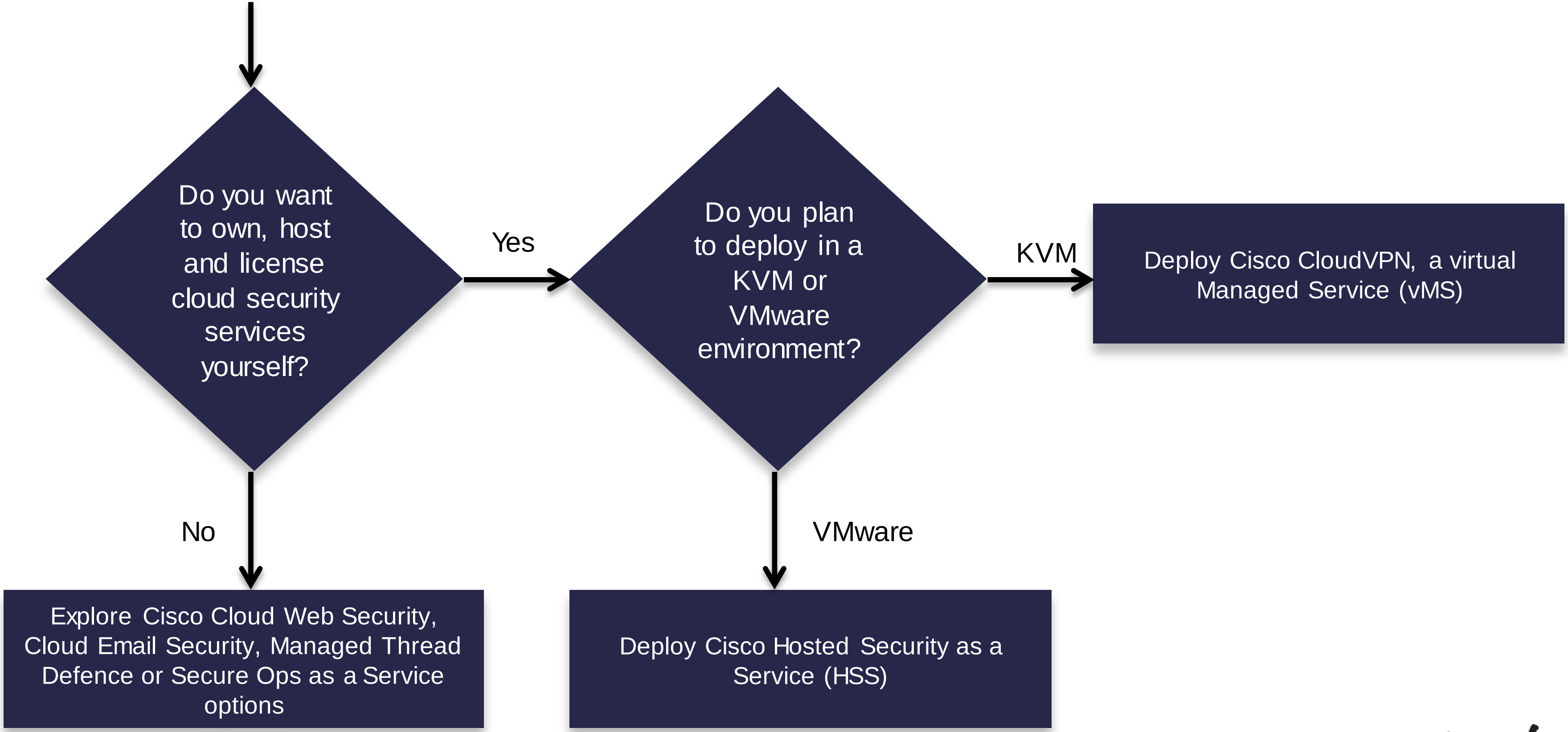
Demo: CloudVPN

Agenda

- Introduction
- The Hosted Security Service Architecture
  - Architecture
  - HSS: Architecture and Demonstration
  - CloudVPN: Architecture and Demonstration
- Conclusion



Cisco Cloud Security Services Solution Guidance



Do you want to own, host and license cloud security services yourself?

Yes

Do you plan to deploy in a KVM or VMware environment?

KVM

Deploy Cisco CloudVPN, a virtual Managed Service (vMS)

VMware

Deploy Cisco Hosted Security as a Service (HSS)

No

Explore Cisco Cloud Web Security, Cloud Email Security, Managed Thread Defence or Secure Ops as a Service options

Summary

- Lower cost due to virtualisation.
- Faster time to service delivery (zero touch deployment, no truck roll), due to virtualisation and service provisioning automation.
- Operational simplicity due to virtualisation.
- Easy upsell for multi-service strategy for additional services and revenue with no additional truck roll.
- Value of multi-service strategy for virtualised managed security services and Cloud hosted services.

Call to Action

- Visit the World of Solutions for
  - Cisco Campus – Security and Service Provider areas
  - Campus Theatre Presentation on Wednesday at 6:30pm by Terri Quinn
- Meet the Expert
- Lunch time Table Topics
- DevNet Zone related labs and sessions
  - CloudVPN
- Recommended Reading:
  - HSS CVD link, www.cisco.com/go/hss
- We want to work with you, please contact us if you need help:
  - Michael Geller – mgeller@cisco.com
  - Albra Welch – albra@cisco.com

Q & A

Complete Your Online Session Evaluation

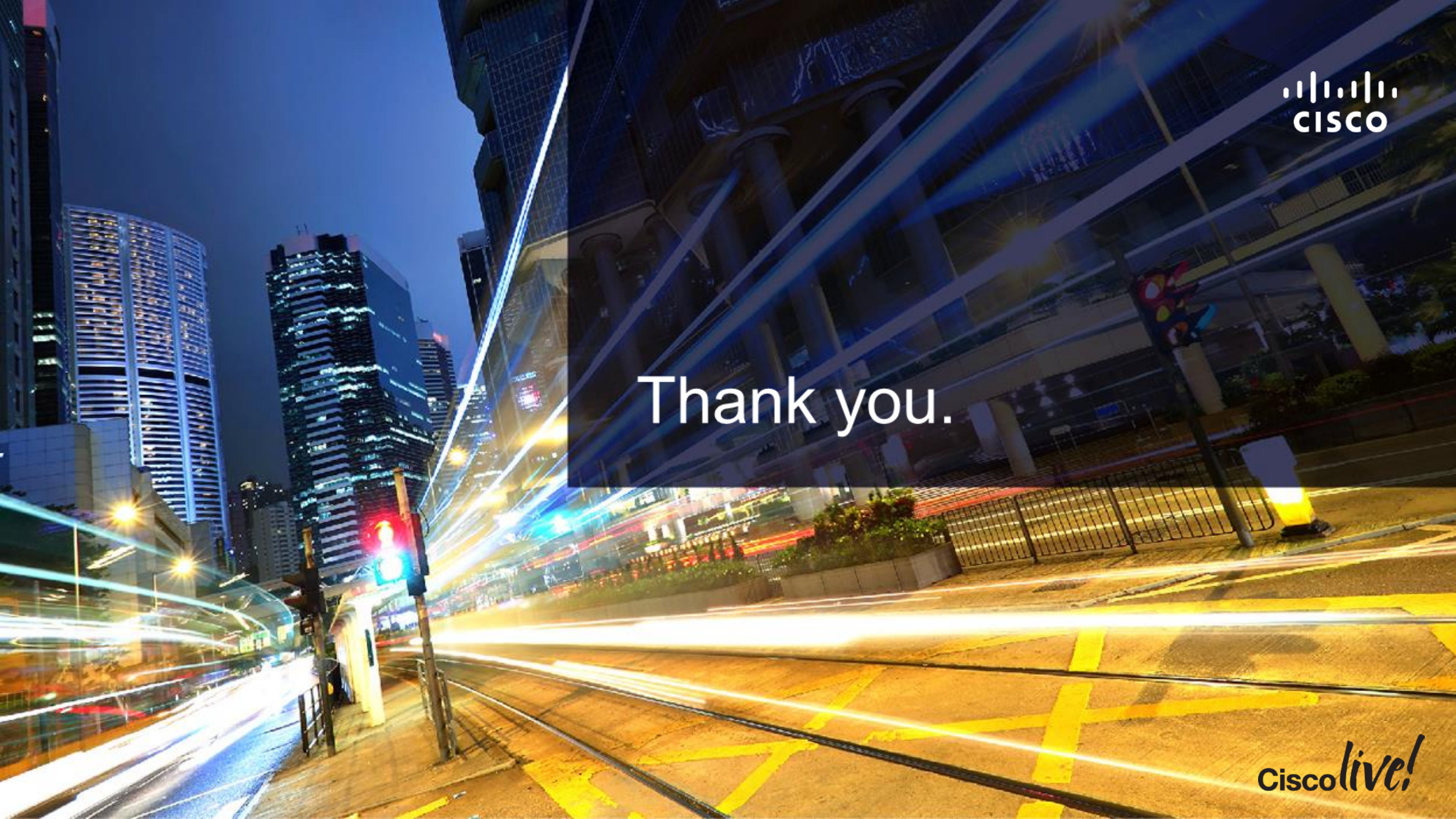
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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 http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com



Thank you.

cisco