
TOMORROW
starts here.
CISCO
Cisco live!

Integration of Hypervisors and L4-7 Services into an ACI Fabric

BRKACI-2006

Bradley Wong
Principal Engineer, INSBU Technical Marketing

#clmel

Cisco live!

“ This session provides a technical introduction to how the ACI fabric handles single and multi-hypervisor environments, how the ACI controller provides integration into different VMMs for a single point of management for virtual network management as well as how the fabric integrates and automates both virtual and physical L4-L7 services…”

BRKACI-2006 ABSTRACT

Agenda

- Introduction to ACI
- Review of ACI Policy Model
- Hypervisor Integration
- Layer 4-7 Services Integration
- Conclusion

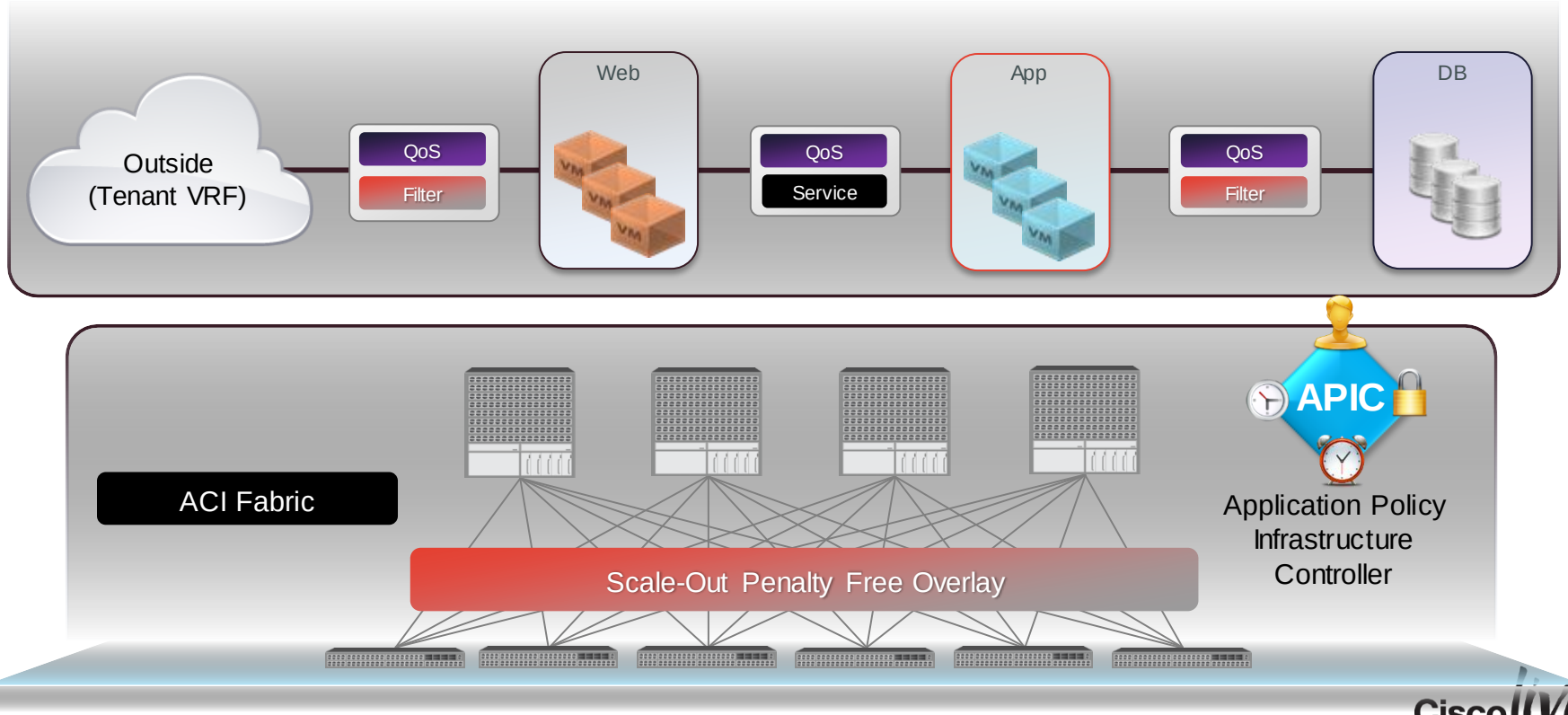
Cisco live!

Introduction to ACI

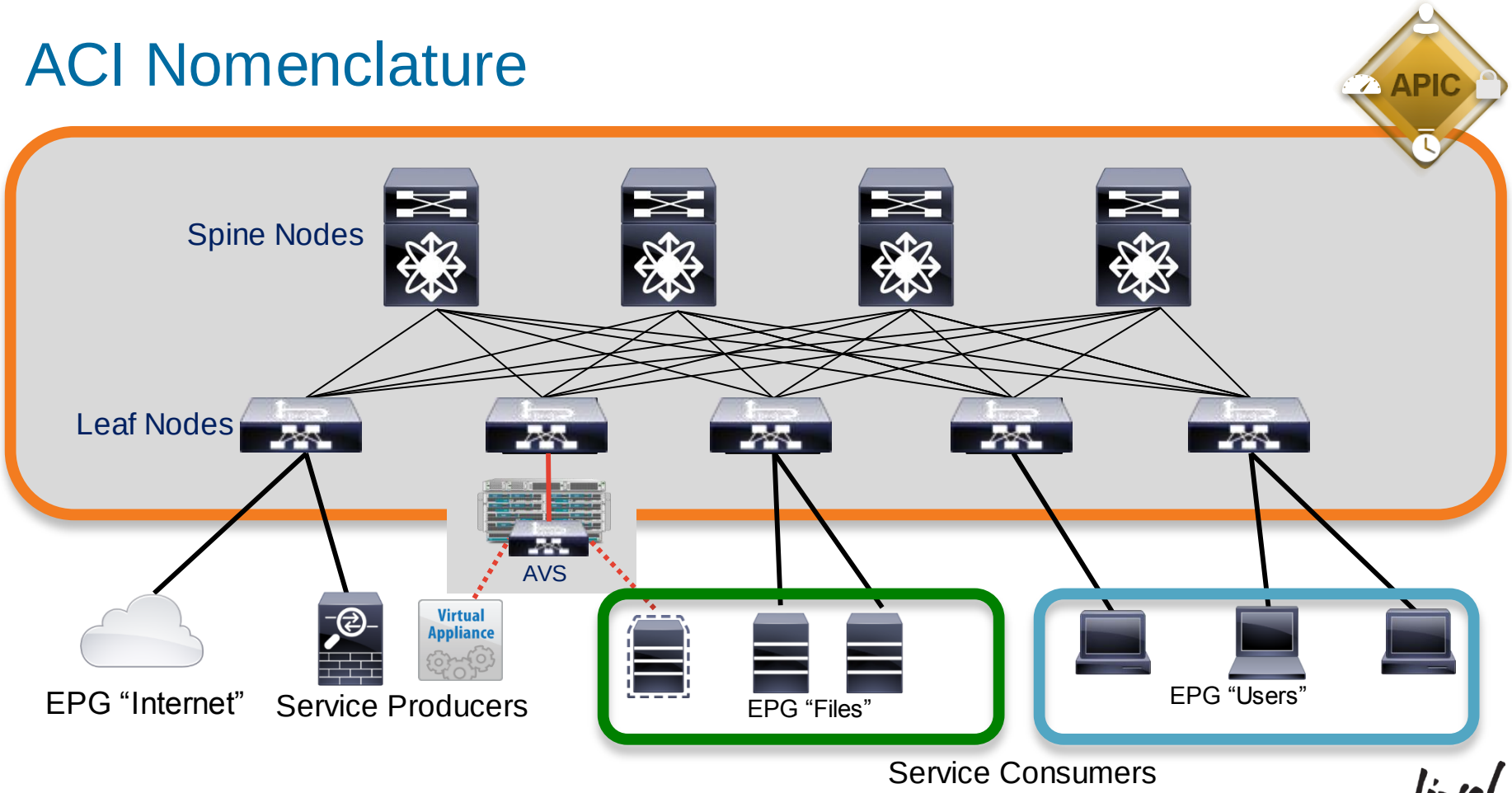
Cisco live!

Cisco ACI

Logical Network Provisioning of Stateless Hardware



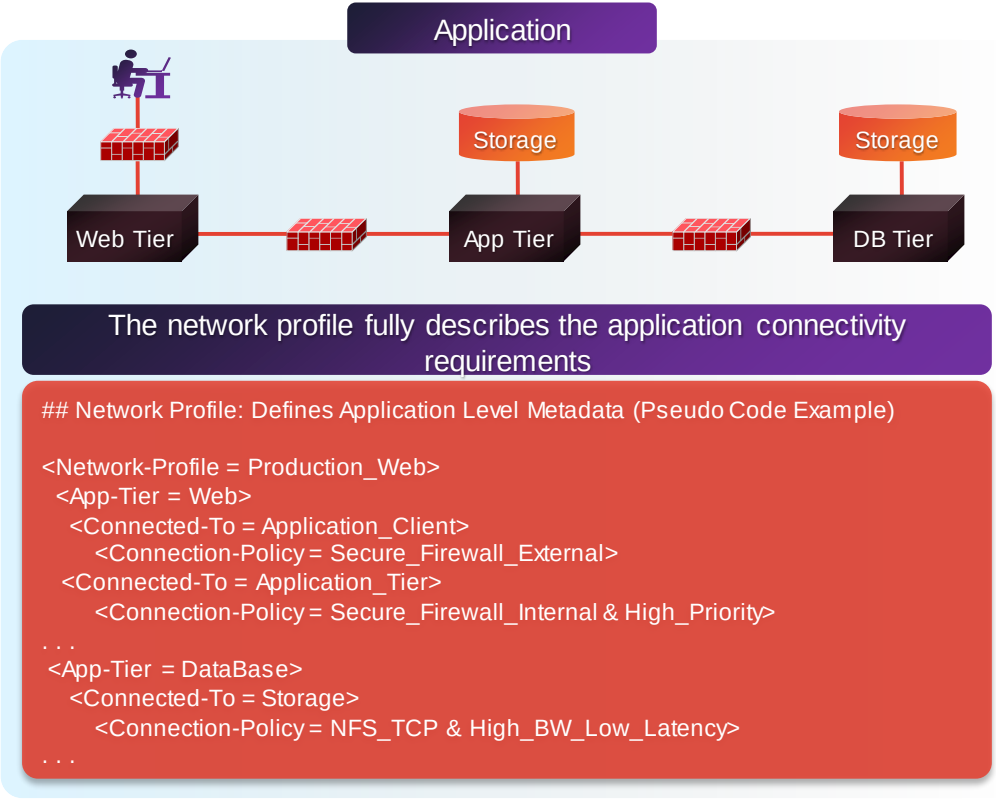
ACI Nomenclature



ACI Network Profile

Policy-Based Fabric Management

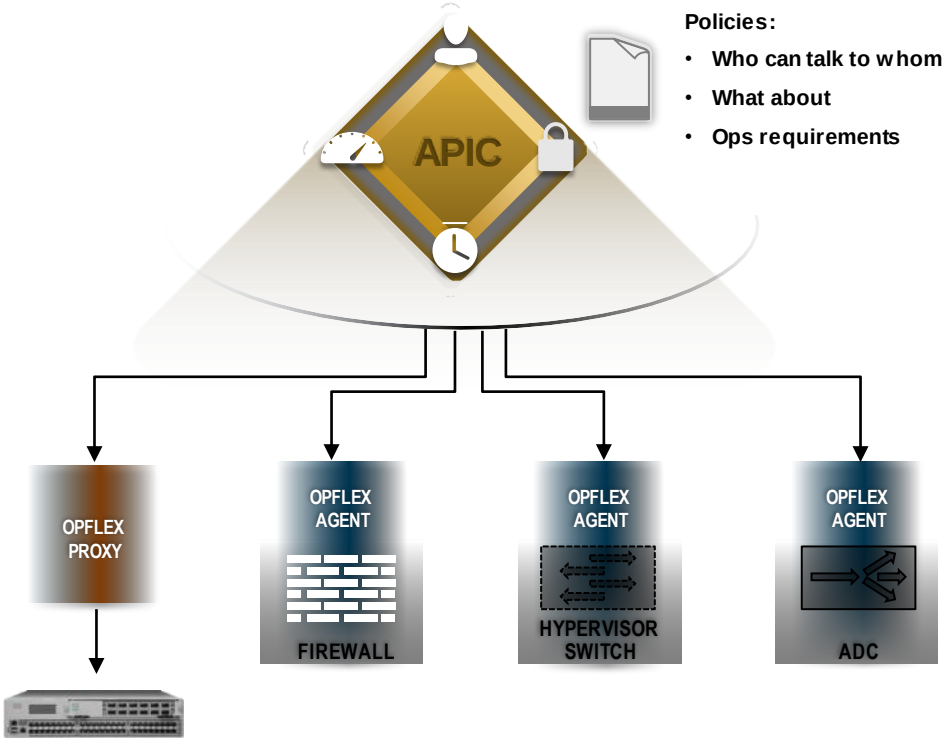
- Extend the principle of Cisco UCS® Manager service profiles to the entire fabric
- Network profile: stateless definition of application requirements
  - Application tiers
  - Connectivity policies
  - Layer 4 – 7 services
  - XML/JSON schema
- Fully abstracted from the infrastructure implementation
  - Removes dependencies of the infrastructure
  - Portable across different data centre fabrics



Opflex: AN OPEN, Extensible Policy Protocol

OPFLEX WAS DESIGNED TO OFFER:

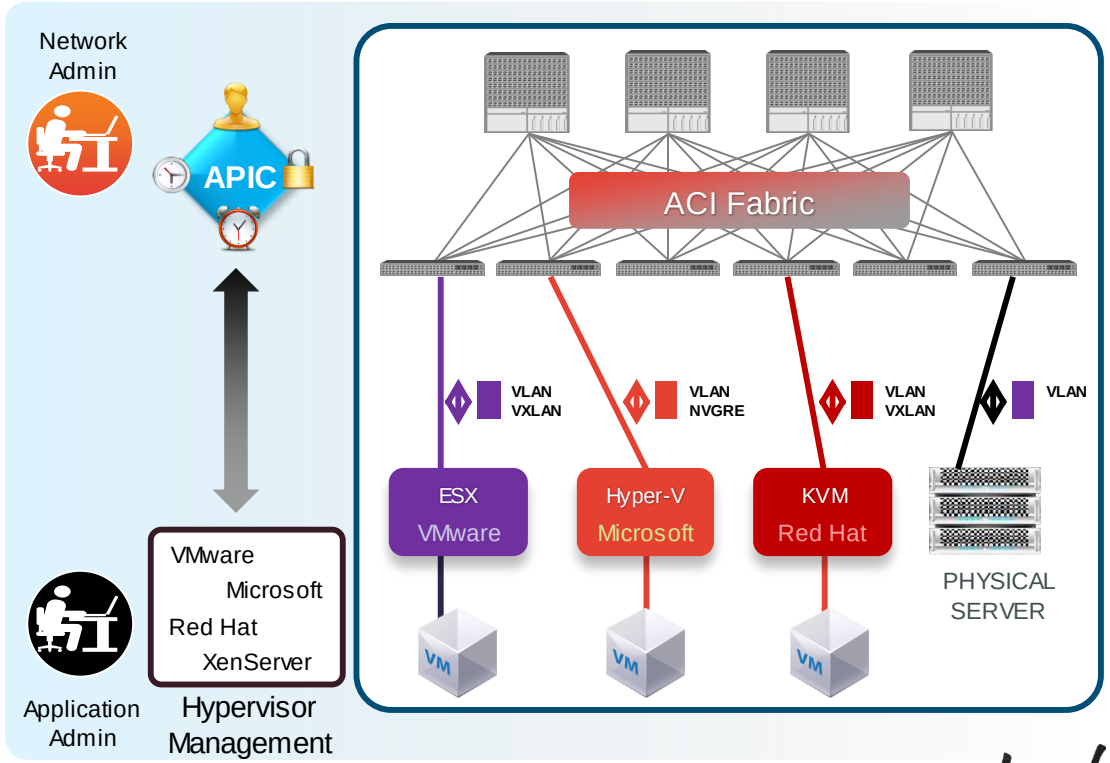
1. Abstract policies rather than device-specific configuration
2. Flexible, extensible definition of using XML / JSON
3. Support for any device including virtual switches, physical switches, network services with strong interoperability across vendors
4. Open, standardised API with an open source reference implementation



Multi-Hypervisor-Ready Fabric

Virtual Integration

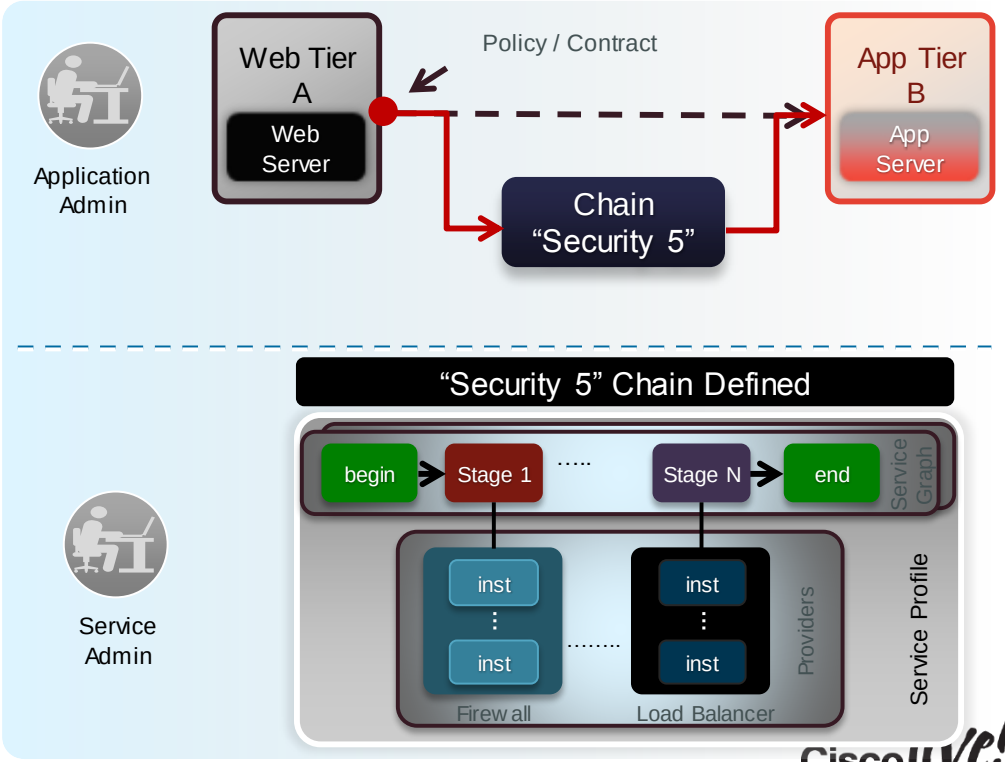
- Integrated gateway for VLAN, VxLAN, and NVGRE networks from virtual to physical
- Normalisation for NVGRE, VXLAN, and VLAN networks
- Customer not restricted by a choice of hypervisor
- Fabric is ready for multi-hypervisor



ACI Layer 4 - 7 Service Integration

Centralised, Automated, And Supports Existing Model

- Elastic service insertion architecture for physical and virtual services
- Helps enable administrative separation between application tier policy and service definition
- APIC as central point of network control with policy coordination
- Automation of service bring-up/tear-down through programmable interface
- Supports existing operational model when integrated with existing services
- Service enforcement guaranteed, regardless of endpoint location

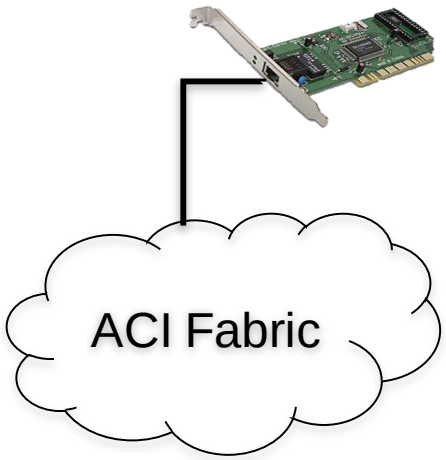


Review of the ACI Policy Model

Cisco live!

End-points

→ Things that connect to the fabric and use it to interface with other things
→ A compute, storage or service instance attaching to a fabric

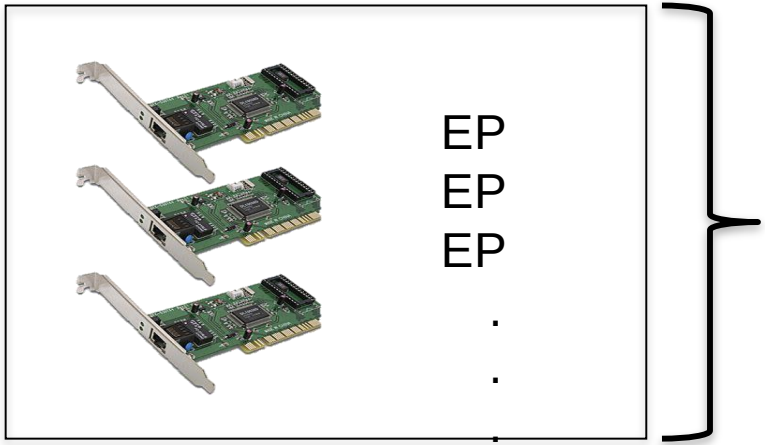


NIC
vNIC
.
.
.

end-points [**EP**]

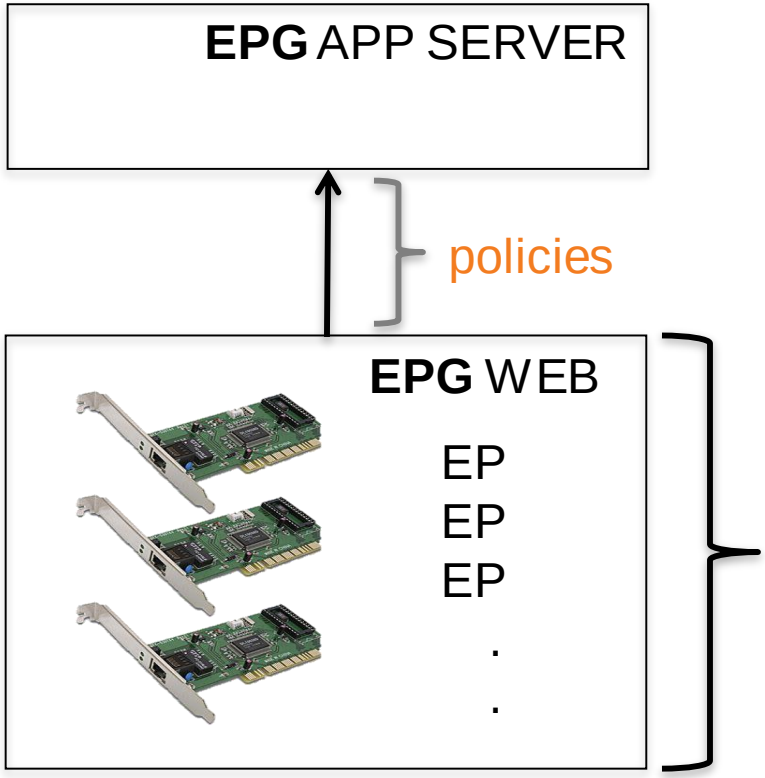
End-points

→ Things that connect to the fabric and use it to interface with other things
→ A compute, storage or service instance attaching to a fabric



A collection of end-points with identical network behaviour form a … ***End Point Group (EPG)***

End-point Groups (EPGs)



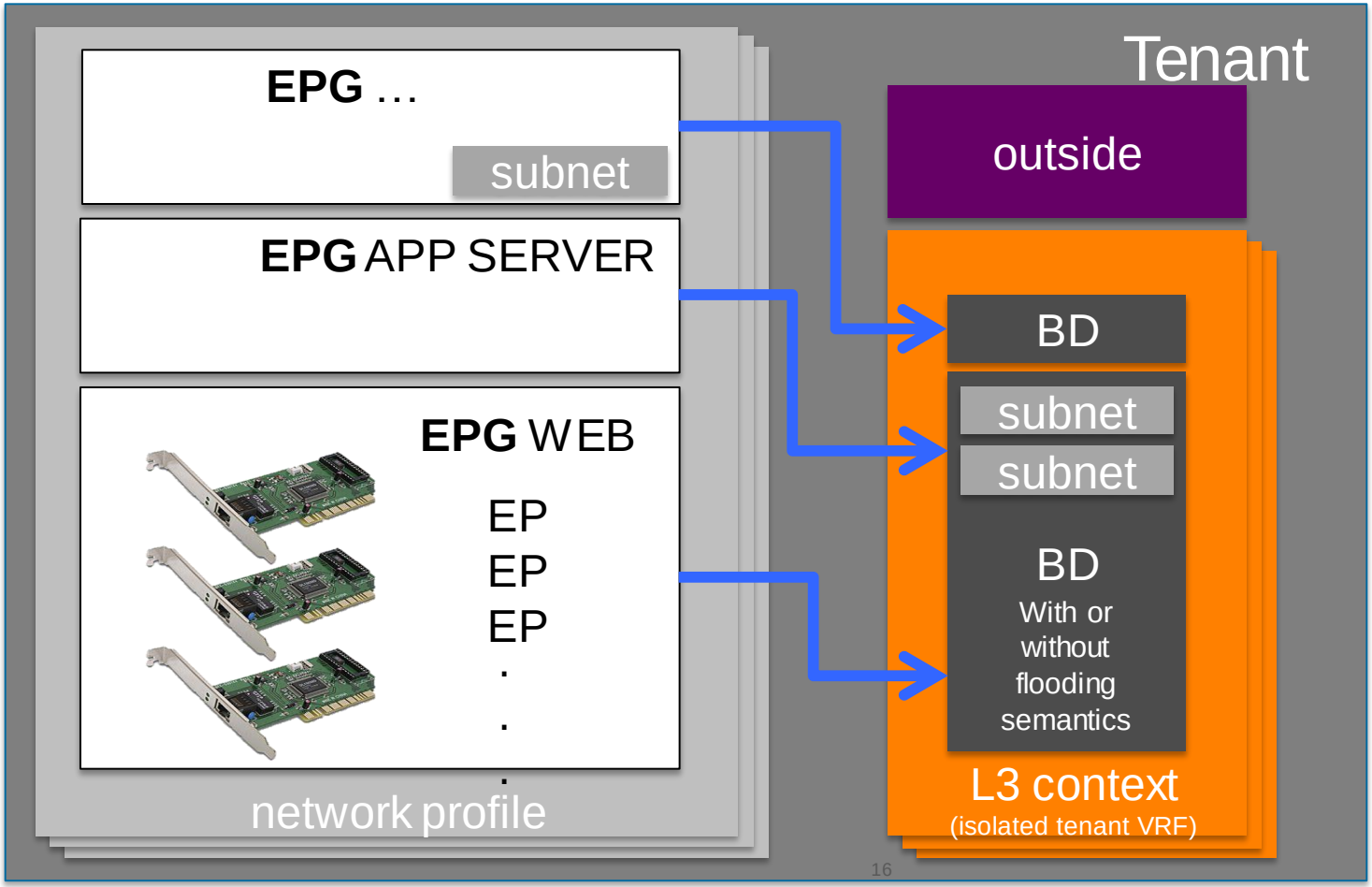
Allows to specify rules and policies on groups of physical or virtual end-points without understanding of specific identifiers and regardless of physical location.

Can flexibly map into

→application tier of multi-tier app
→segmentation construct (ala VLAN)
→a security construct
→ESX port group, SCVMM VMNetwork
→…

… **end-point group** [***EPG***]

Tenant L3, L2 Isolation



self-contained tenant definition representable as a recursive structured text document

Integration with Multiple Hypervisors

Cisco live!

Hypervisor Integration Agenda

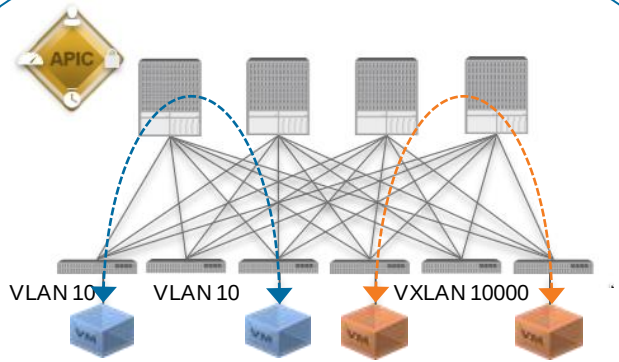
- Hypervisor Integration Overview
- VMWare vCenter Integration
- Microsoft SCVMM & Azure Pack Integration
- OpenStack Integration

Cisco live!

Hypervisor Interaction with ACI

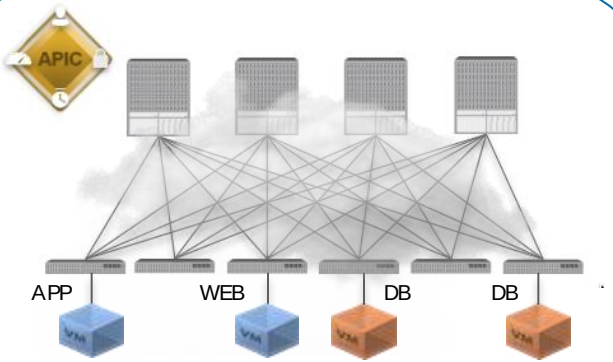
Two modes of Operation

Non-Integrated Mode



- ACI Fabric as an IP-Ethernet Transport
- Encapsulations manually allocated
- Separate Policy domains for Physical and Virtual

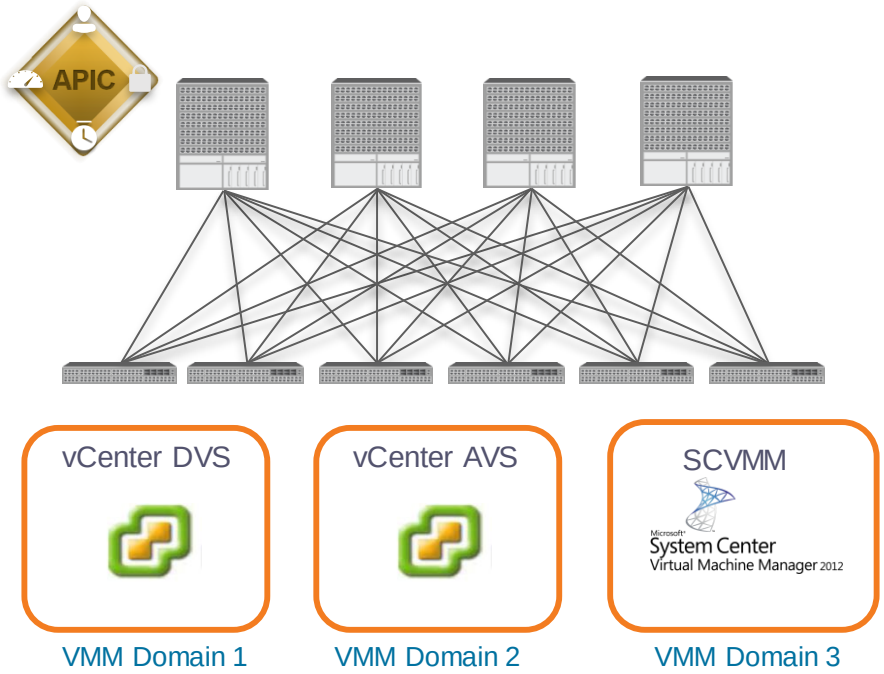
Integrated Mode



- ACI Fabric as a Policy Authority
- Encapsulations Normalised and dynamically provisioned
- Integrated Policy domains across Physical and Virtual

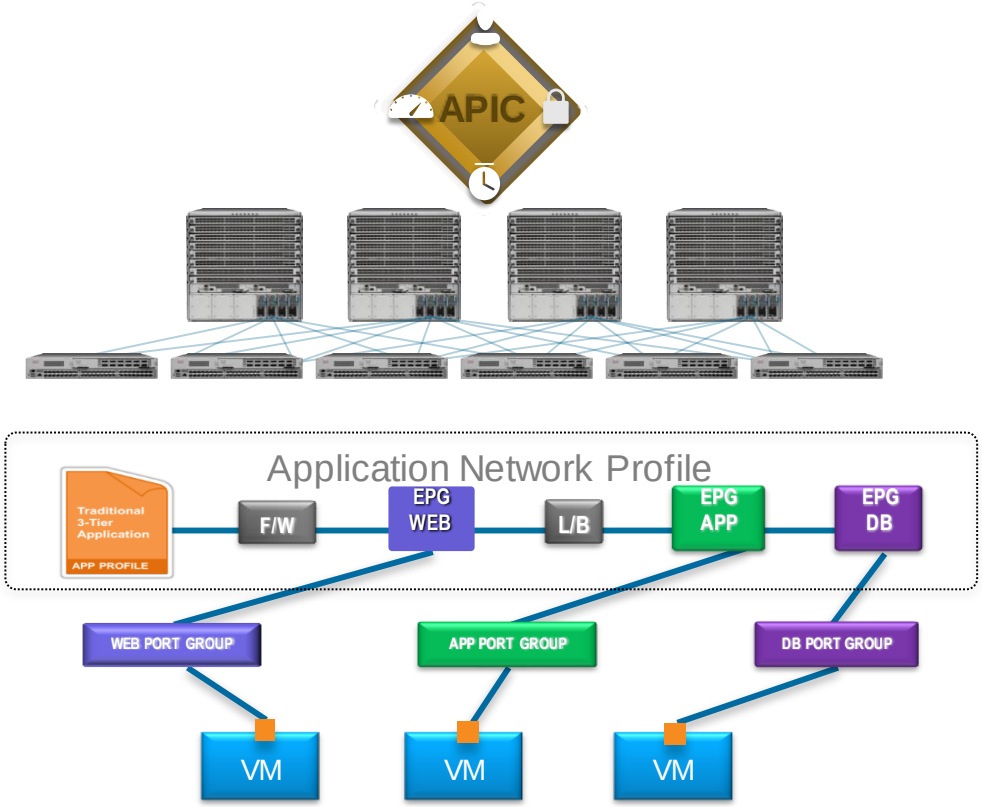
Hypervisor Integration with ACI

Control Channel - VMM Domains



- Relationship is formed between APIC and Virtual Machine Manager (VMM)
- Multiple VMMs likely on a single ACI Fabric
- Each VMM and associated Virtual hosts are grouped within APIC
- Called VMM Domain
- There is 1:1 relationship between a Virtual Switch and VMM Domain

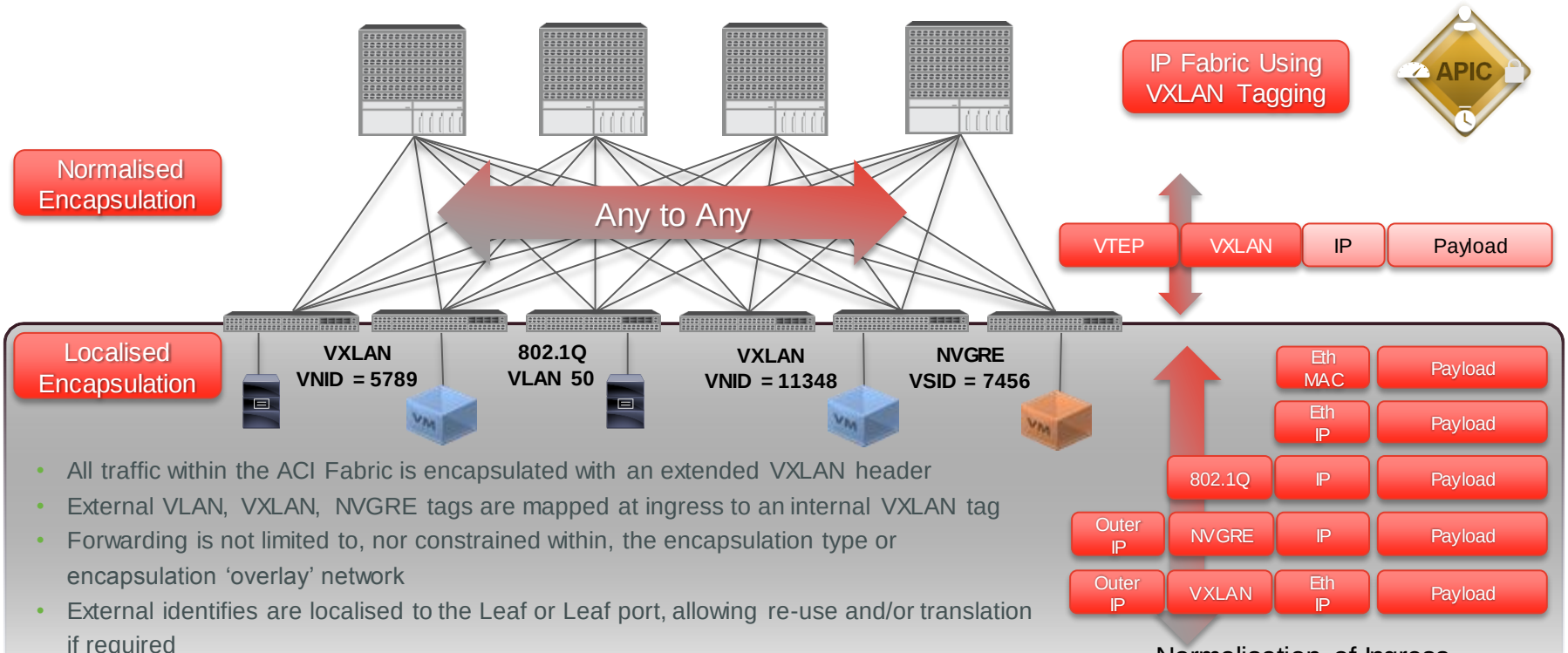
Hypervisor Integration with ACI



- ACI Fabric implements policy on Virtual Networks by mapping Endpoints to EPGs
- Endpoints in a Virtualised environment are represented as the vNICs
- VMM applies network configuration by placement of vNICs into Port Groups or VM Networks
- EPGs are exposed to the VMM as a 1:1 mapping to Port Groups or VM Networks

ACI Fabric – Integrated Overlay

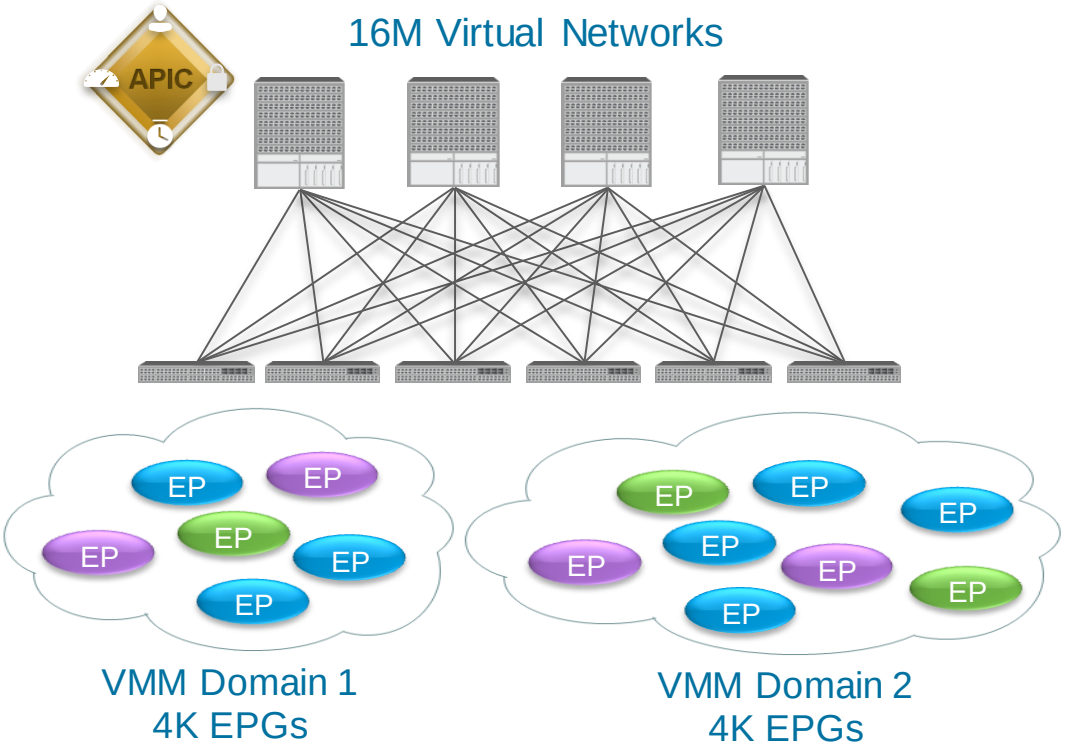
Data Path - Encapsulation Normalisation



- All traffic within the ACI Fabric is encapsulated with an extended VXLAN header
- External VLAN, VXLAN, NVGRE tags are mapped at ingress to an internal VXLAN tag
- Forwarding is not limited to, nor constrained within, the encapsulation type or encapsulation 'overlay' network
- External identifies are localised to the Leaf or Leaf port, allowing re-use and/or translation if required

Hypervisor Integration with ACI

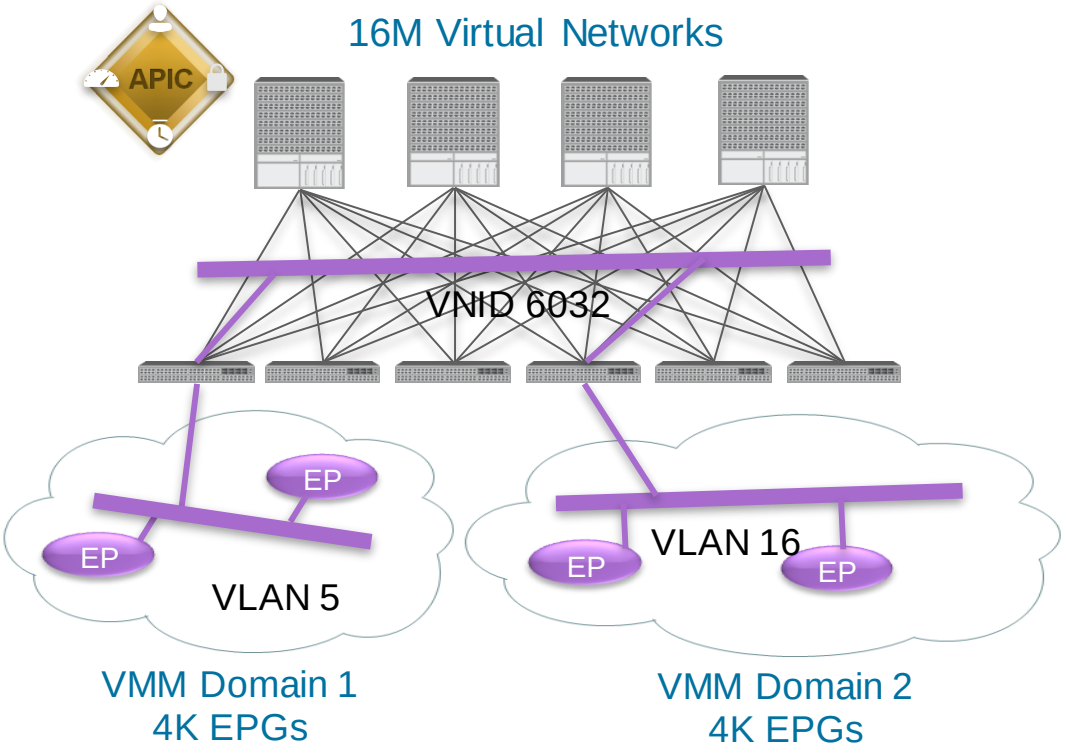
VMM Domains & VLAN Encapsulation



- VLAN ID only gives 4K EPGs (12 bits)
- Scale by creating **pockets** of 4K EPGs
- Map EPGs to VMM Domain based on scope of live migration
- Place VM anywhere
- Live migrate within VMM domain

Hypervisor Integration with ACI

VMM Domains & VLAN Encapsulation

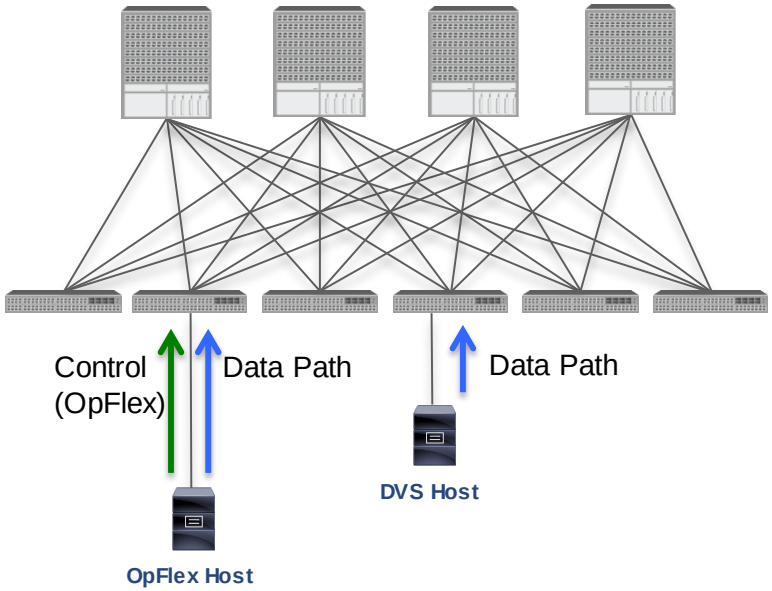


- VLAN ID only gives 4K EPGs (12 bits)
- Scale by creating **pockets** of 4K EPGs
- Map EPGs to VMM Domain based on scope of live migration
- Place VM anywhere
- Live migrate within VMM domain

Hypervisor Integration with ACI

Endpoint Discovery

- Virtual Endpoints are discovered for reachability & policy purposes via 2 methods:
- Control Plane Learning:
  - Out-of-Band Handshake: vCenter APIs
  - Inband Handshake: OpFlex-enabled Host (AVS, Hyper-V, etc.)
- Data Path Learning: Distributed switch learning
- LLDP used to resolve Virtual host ID to attached port on leaf node (non-OpFlex Hosts)



Control
(vCenter API)

VMM

Hypervisor Integration Agenda

- Hypervisor Integration Overview
- VMWare vCenter Integration
- Microsoft SCVMM & Azure Pack Integration
- OpenStack Integration

VMWare Integration

Three Different Options

Distributed Virtual Switch (DVS)

- Encapsulations: VLAN
- Installation: Native
- VM discovery: LLDP
- Software/Licenses: vCenter with Enterprise+ License

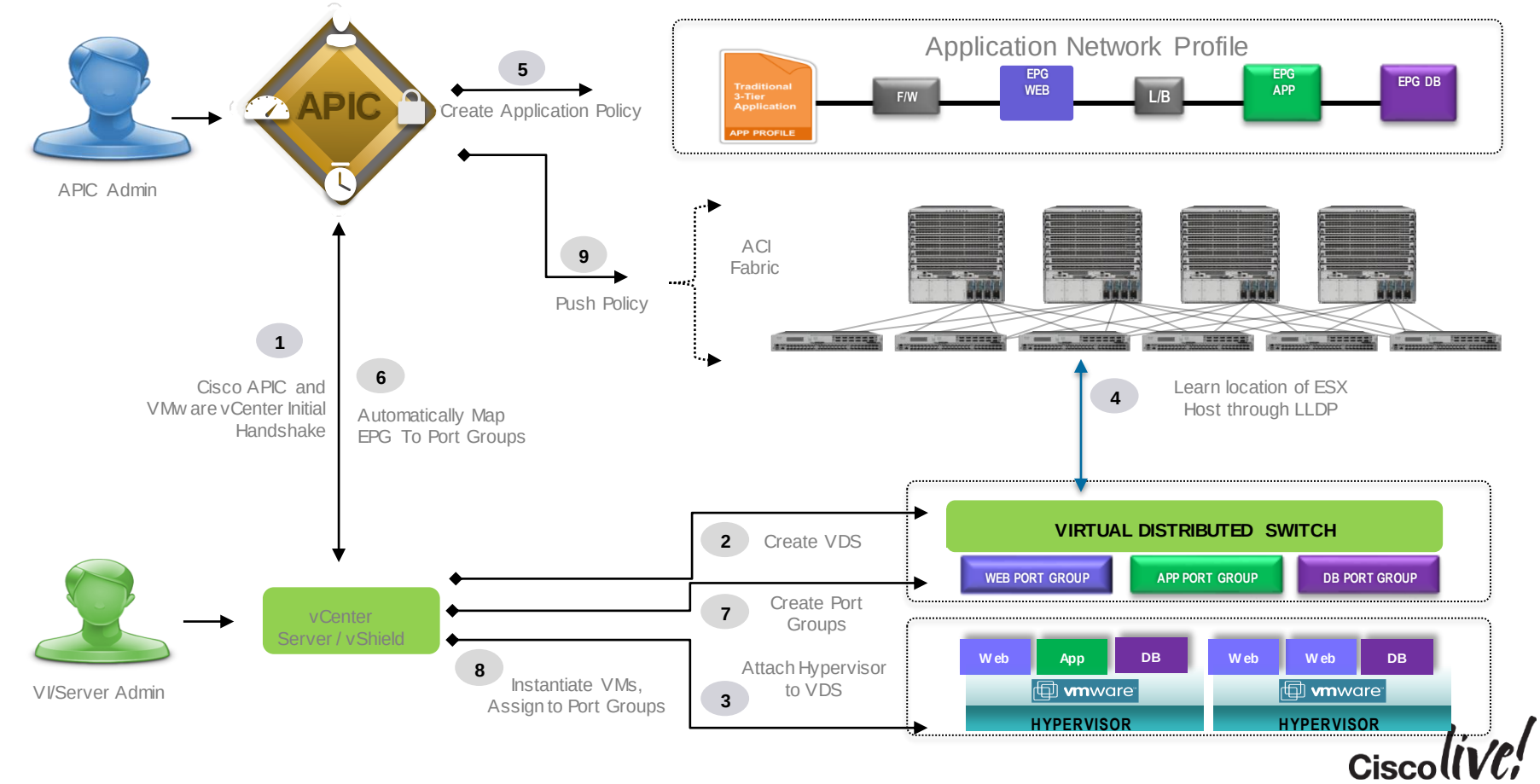
vCenter + vShield

- Encapsulations: VLAN, VXLAN
- Installation: Native
- VM discovery: LLDP
- Software/Licenses: vCenter with Enterprise+ License, vShield Manager with vShield License

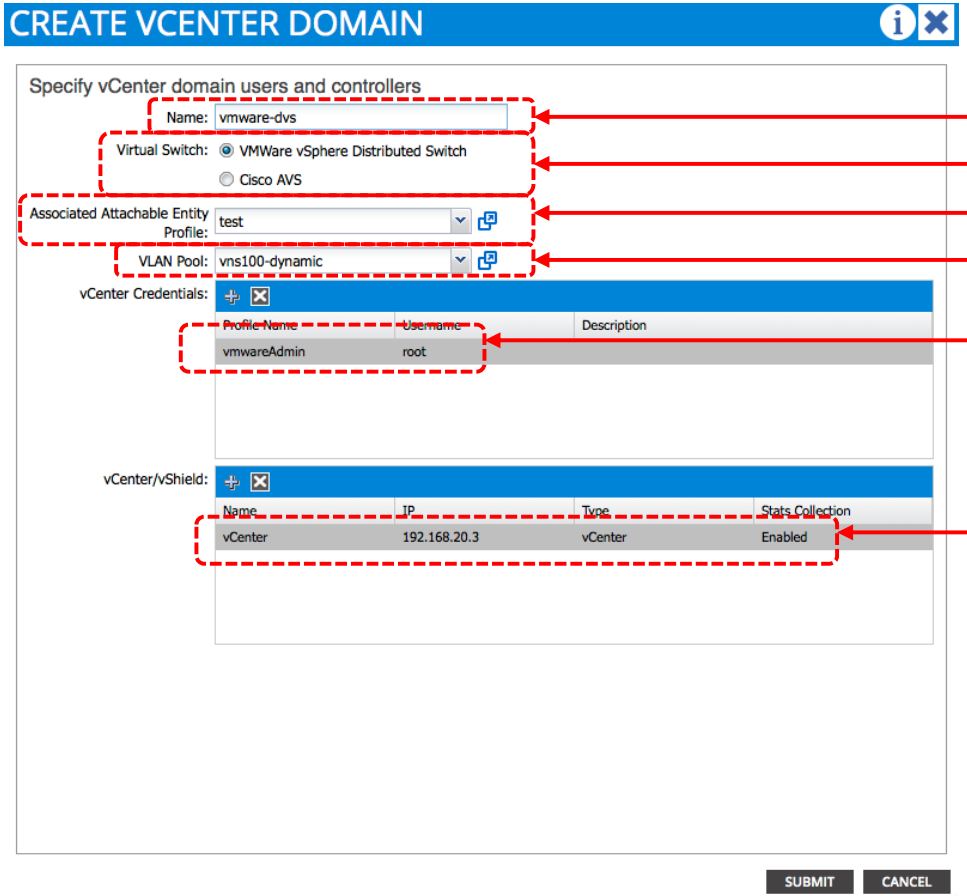
Application Virtual Switch (AVS)

- Encapsulations: VLAN, VXLAN
- Installation: VIB through VUM or Console
- VM discovery: OpFlex
- Software/Licenses: vCenter with Enterprise+ License

ACI Hypervisor Integration – VMware DVS/vShield



ACI Hypervisor Integration – VMware DVS



Name of VMM Domain

Type of vSwitch (DVS or AVS)

Associated Attachable Entity Profile (AEP)

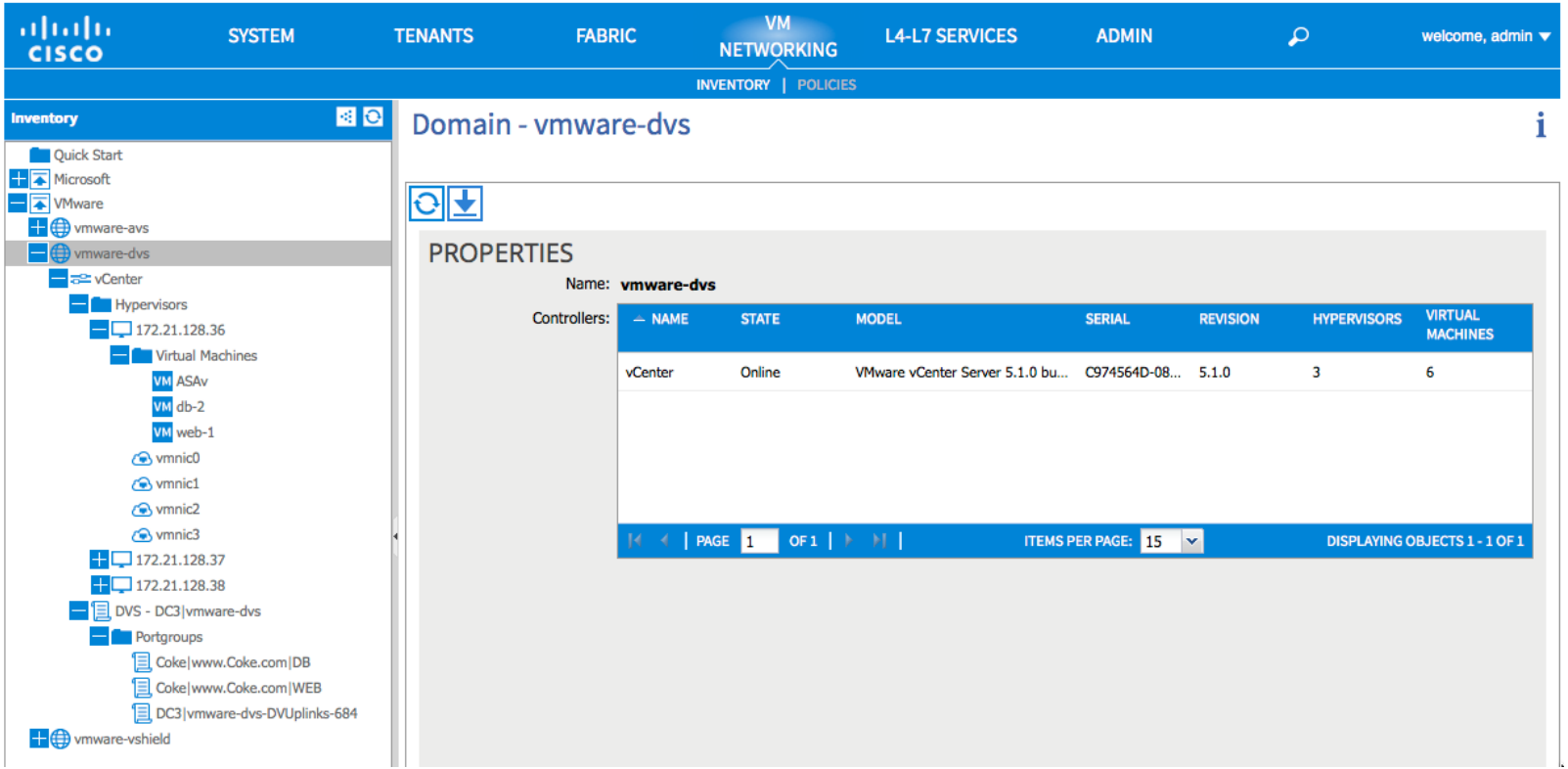
VLAN Pool

vCenter Administrator Credentials

vCenter server information

Cisco live!

ACI Hypervisor Integration – VMware DVS

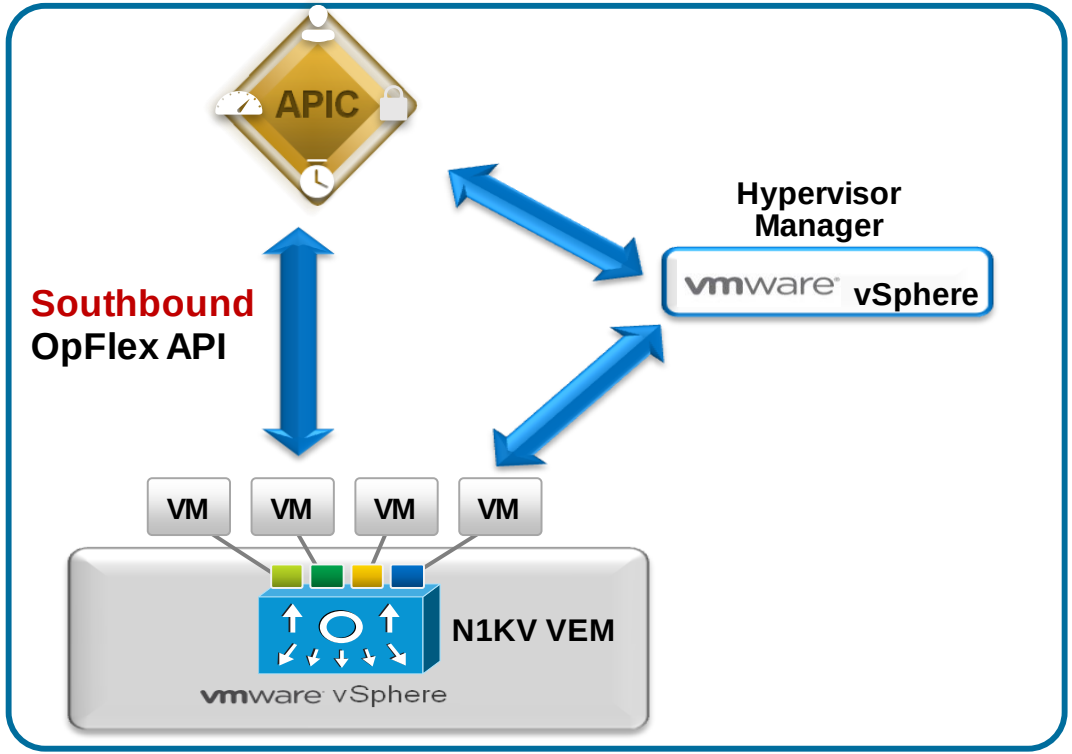


Cisco live!

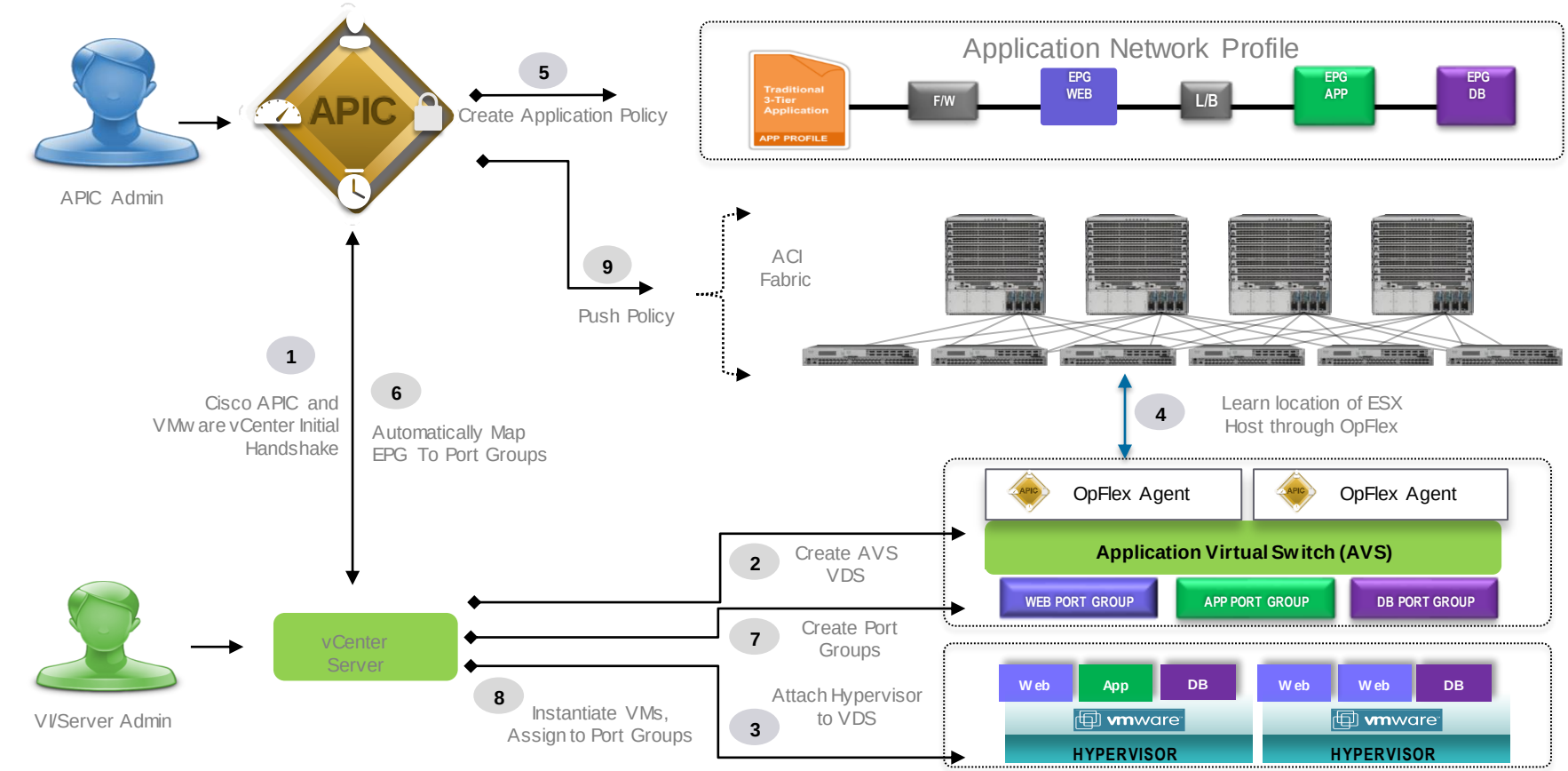
Application Virtual Switch (AVS)

Integration Overview

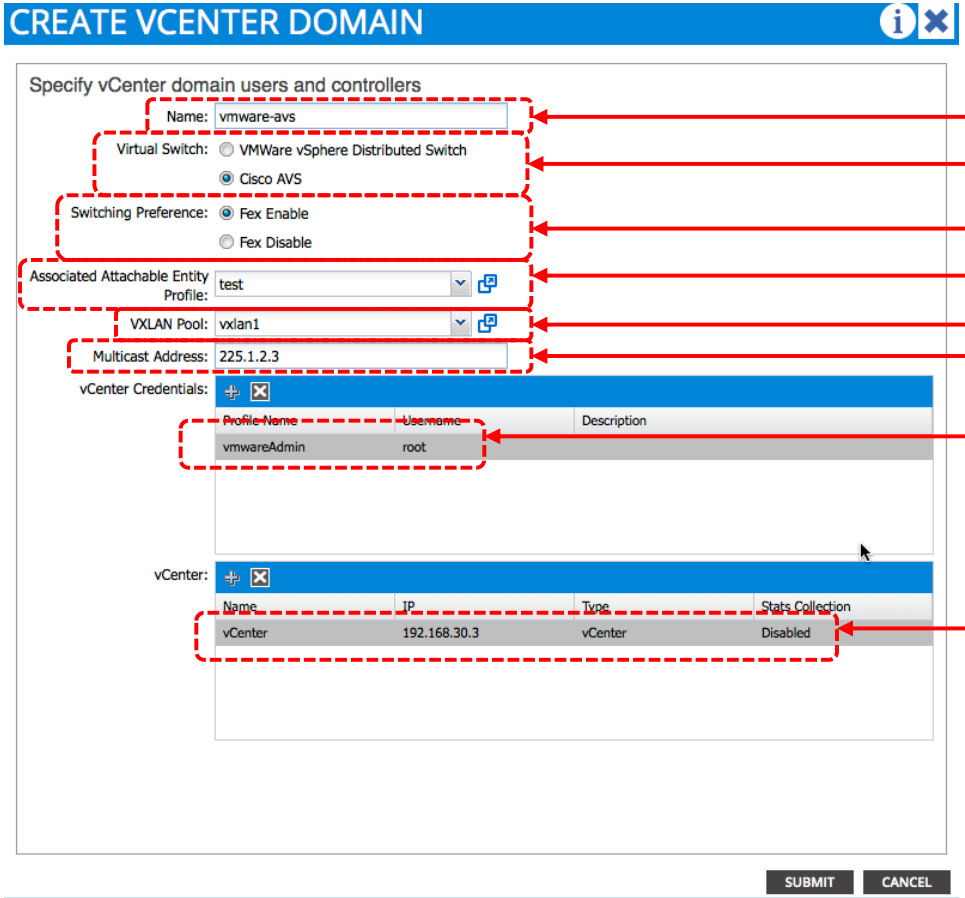
- OpFlex Control protocol
  - Control channel
  - VM attach/detach, link state notifications
- VEM extension to the fabric
- vSphere 5.0 and above
- BPDU Filter/BPDU Guard
- SPAN/ERSPAN
- Port level stats collection
- Remote Virtual Leaf Support (future)



ACI Hypervisor Integration – AVS



ACI Hypervisor Integration – VMware DVS



Name of VMM Domain

Type of vSwitch (DVS or AVS)

Switching mode (FEX or Normal)

Associated Attachable Entity Profile (AEP)

VXLAN Pool

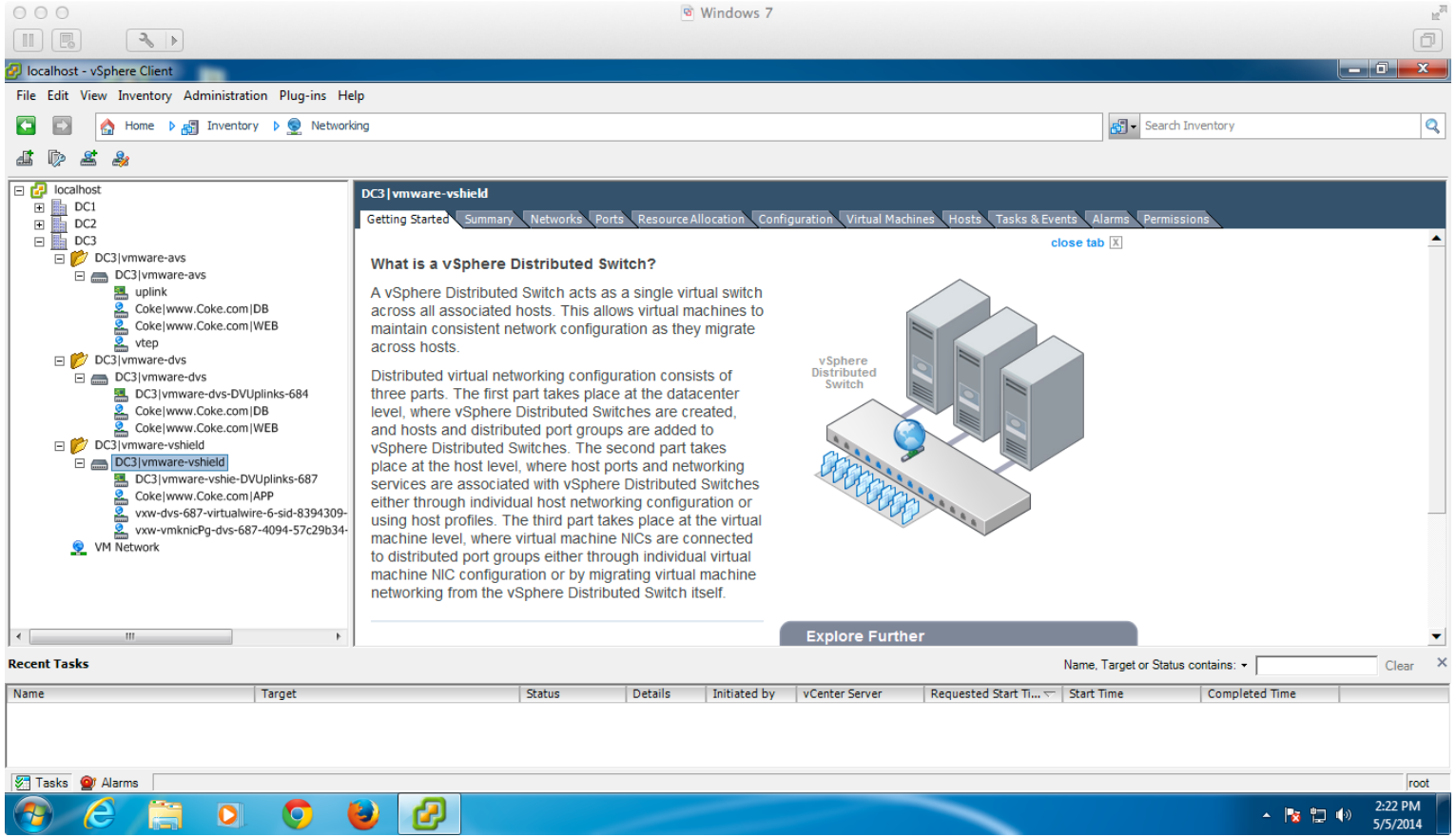
Multicast Pool

vCenter Administrator Credentials

vCenter server information

Cisco live!

ACI Hypervisor Integration – VMware



Hypervisor Integration Agenda

- Hypervisor Integration Overview
- VMWare vCenter Integration
- Microsoft SCVMM & Azure Pack Integration
- OpenStack Integration

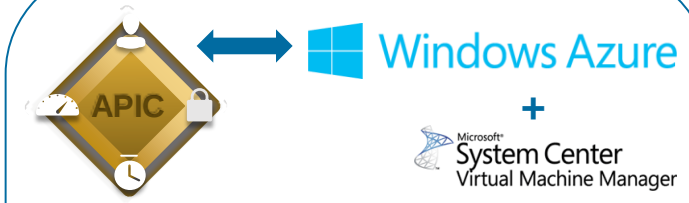
Microsoft Interaction with ACI

Two modes of Operation

Integration with SCVMM

- Policy Management: Through APIC
- Software / License: Windows Server with HyperV, SCVMM
- VM Discovery: OpFlex
- Encapsulations: VLAN, NVGRE (Future)
- Plugin Installation: Manual

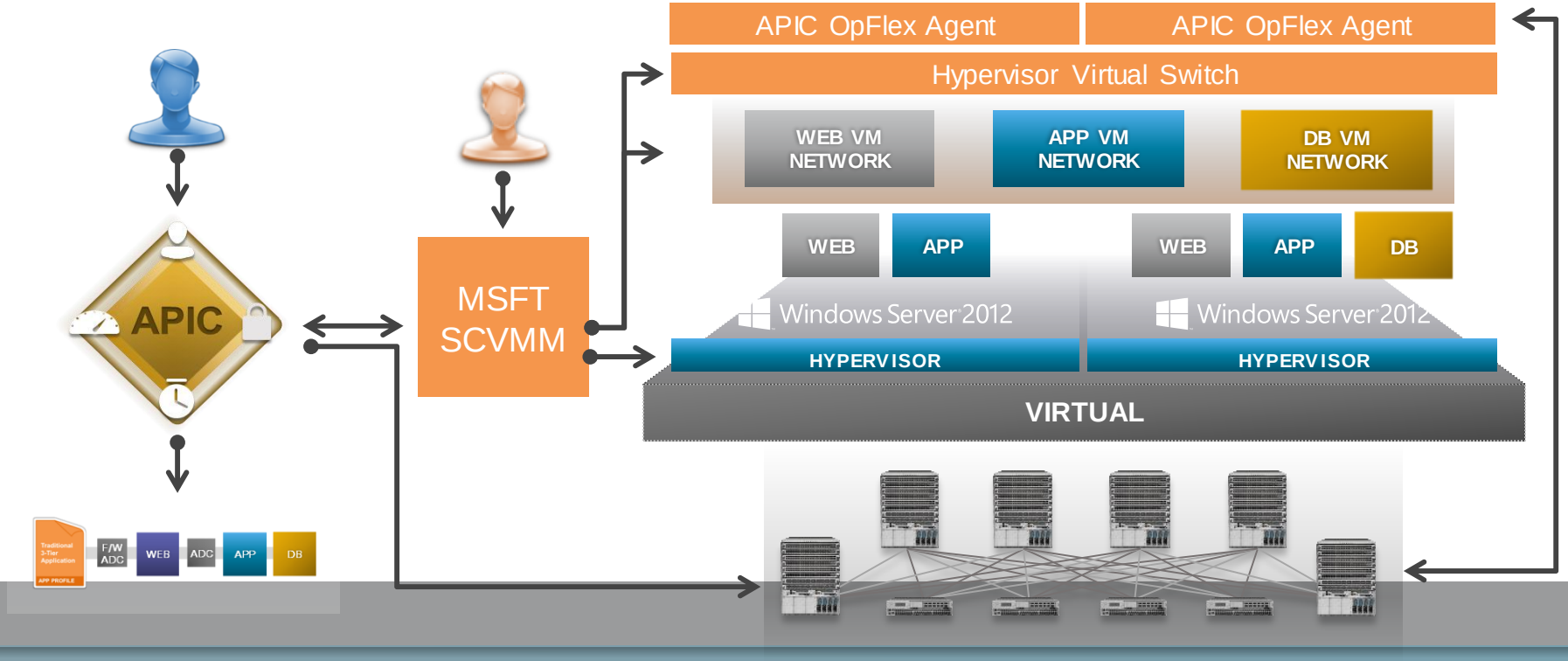
Integration with Azure Pack



- Superset of SCVMM
- Policy Management: Through APIC or through Azure Pack
- Software / License: Windows Server with HyperV, SCVMM, Azure Pack (free)
- VM Discovery: OpFlex
- Encapsulations: VLAN, NVGRE (Future)
- Plugin Installation: Integrated

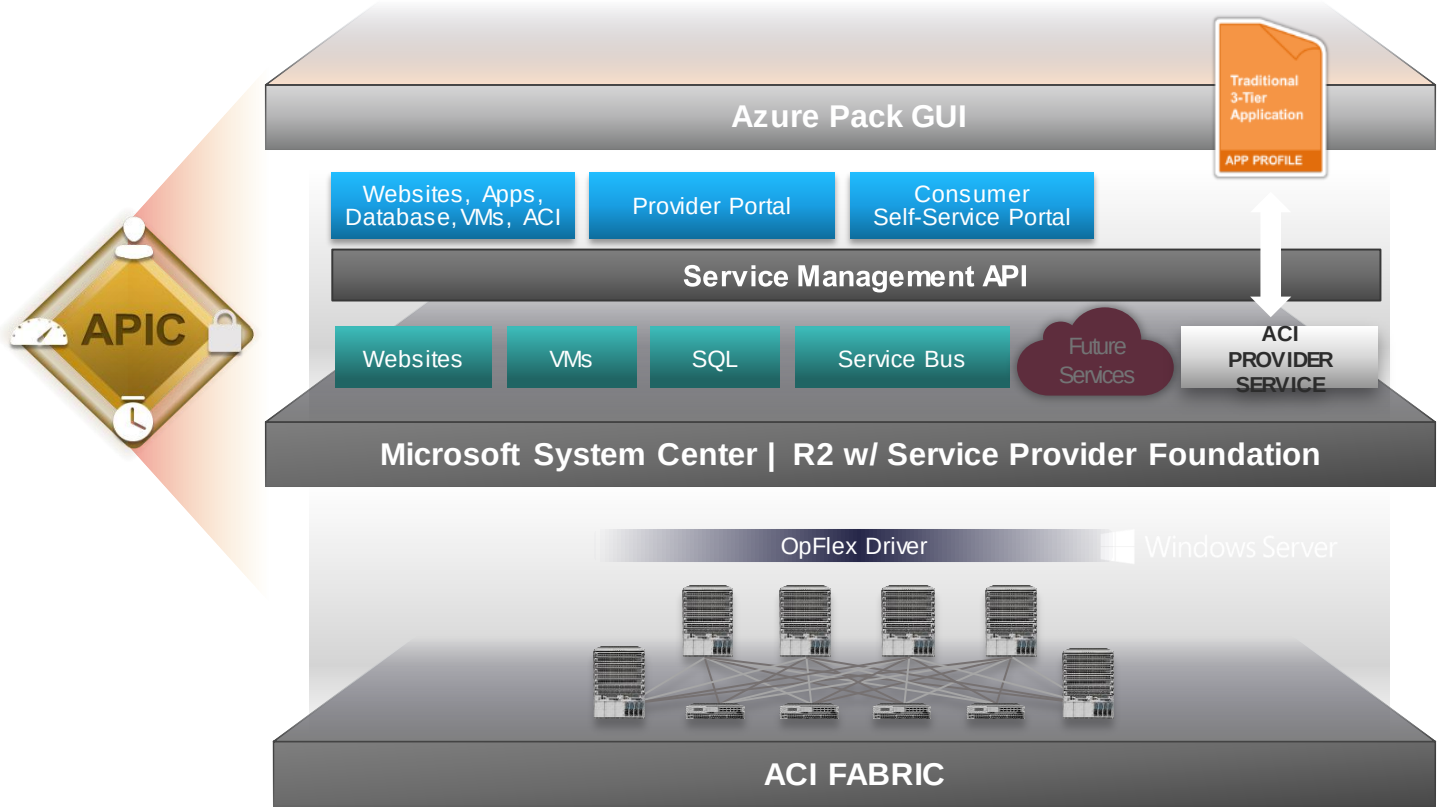
ACI Hypervisor Integration—MSFT SCVMM

Q2 CY 15



Cisco ACI: Microsoft Azure Pack Integration

Q2 CY 15



Policy Management: APIC / Azure Pack

VM Discovery: OpFlex

Encapsulation: VLAN in Q2 CY15

(VXLAN, NVGRE in future)

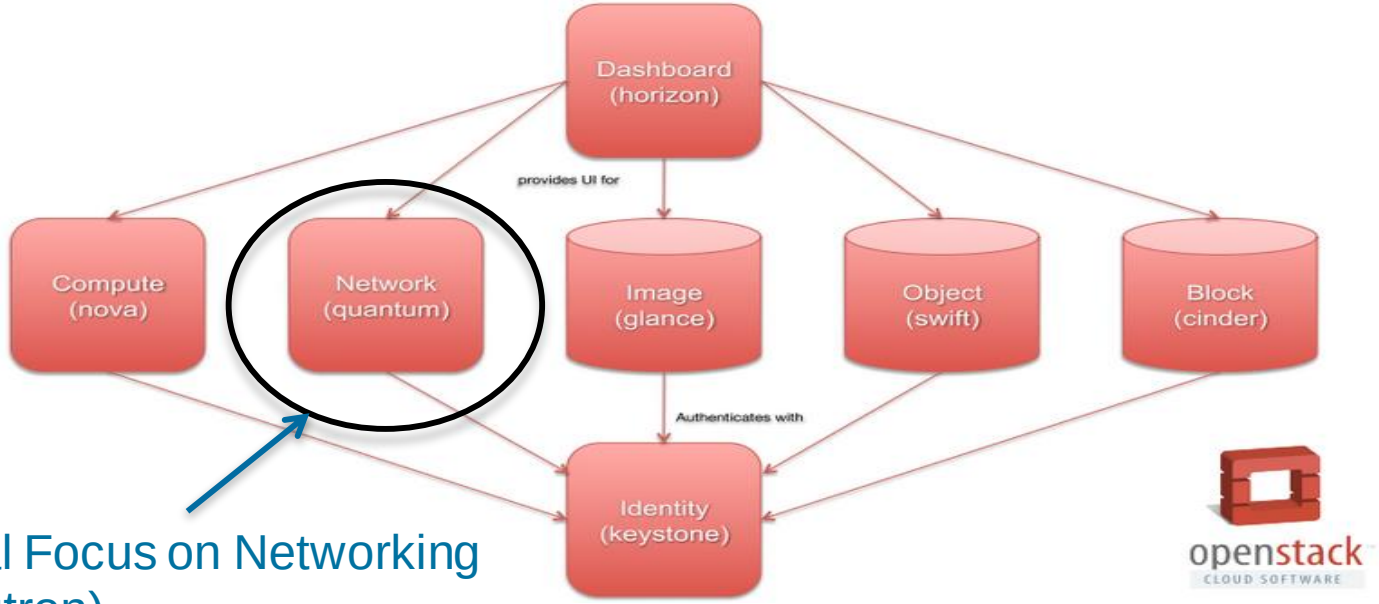
Zero touch network

Service Insertion (Physical/ Virtual)

Hypervisor Integration Agenda

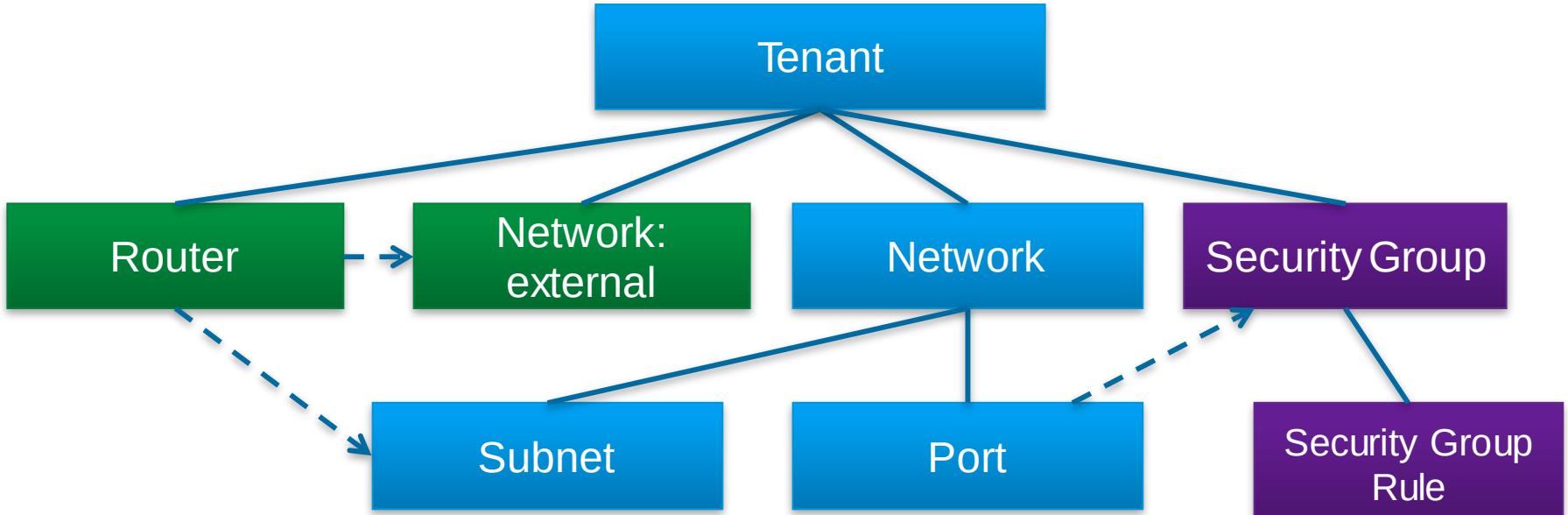
- Hypervisor Integration Overview
- VMWare vCenter Integration
- Microsoft SCVMM & Azure Pack Integration
- OpenStack Integration

OpenStack Components



Initial Focus on Networking (Neutron)

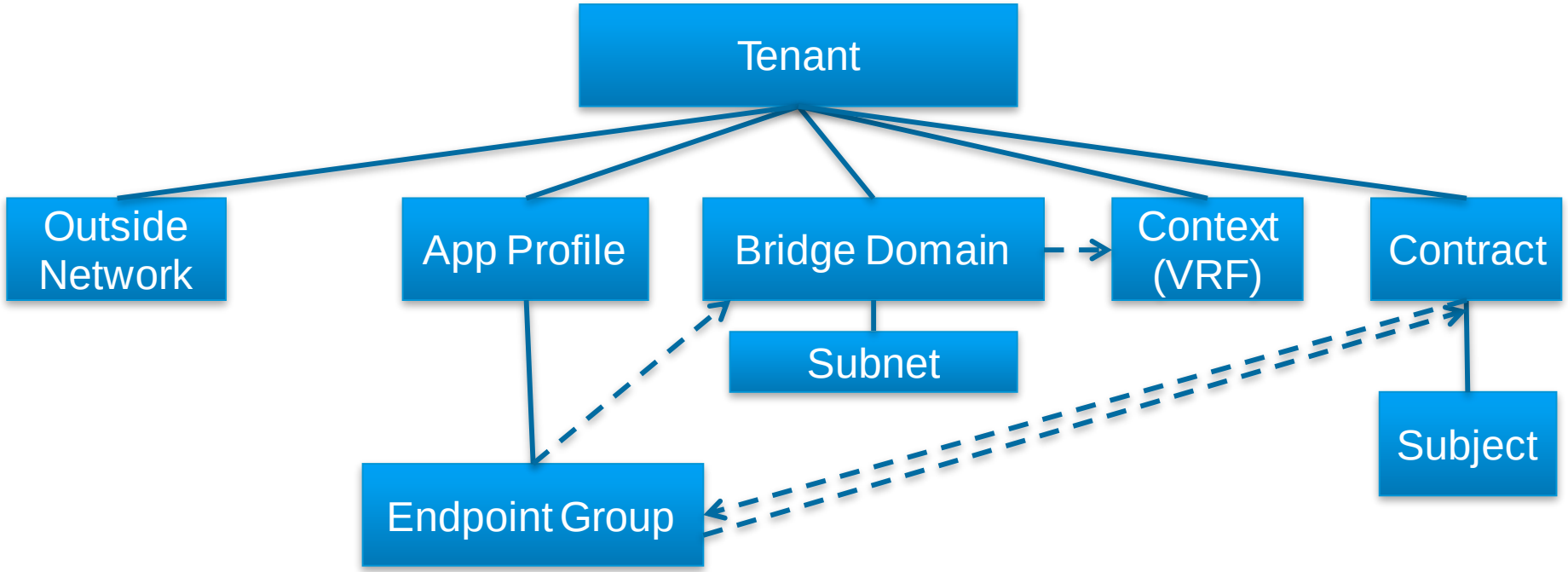
OpenStack Neutron Networking Model



L3 + External Net Extension | Core API | Sec Grp Extension

Cisco live!

Cisco ACI Model

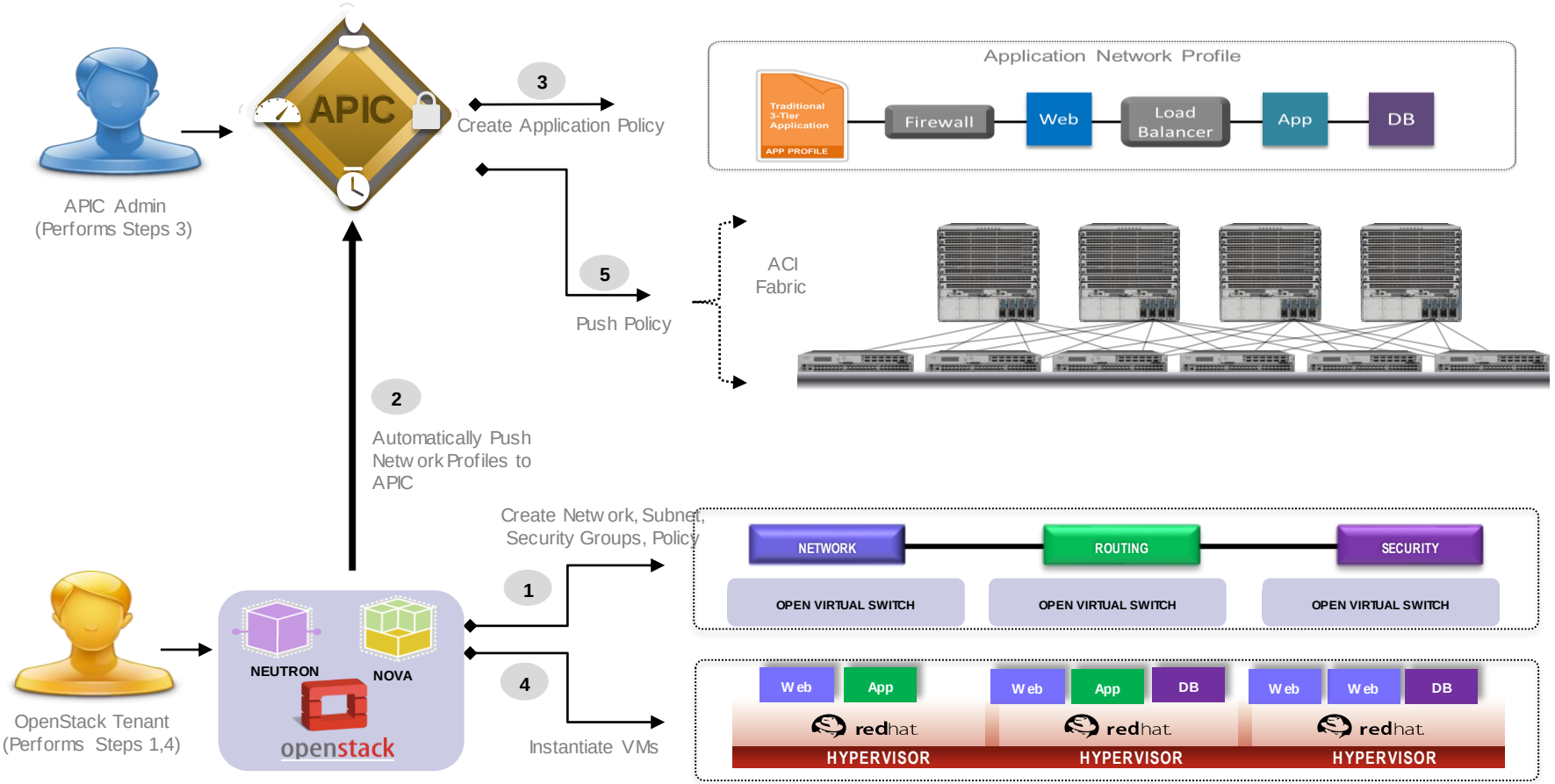


Cisco OpenStack ACI Model

Neutron API Mapping

OpenStack	ACI
Tenant	Tenant
No Equivalent	Application Profile
Network	EPG + Bridge Domain
Subnet	Subnet
Security Group	Handled by Host
Security Group Rule	Handled by Host
Router	L3 Context
Network:External	L3 Outside

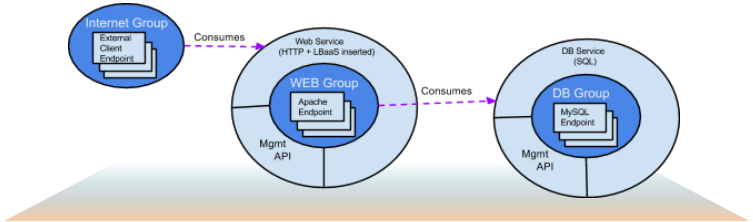
ACI OpenStack Integration – Phase 1



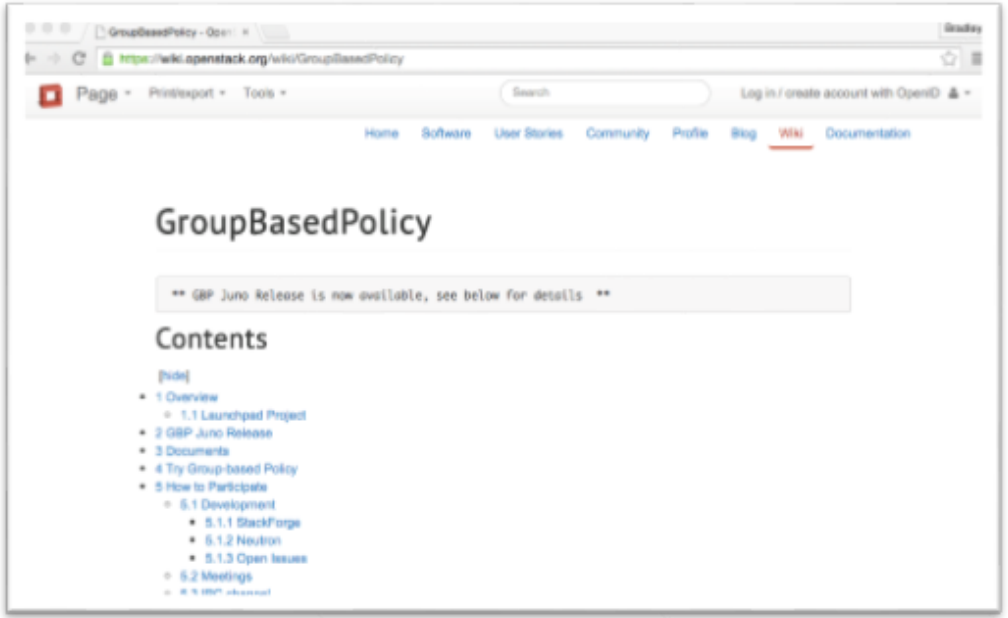
Group-Based Policy in OpenStack

GBP release 2014.2 "Juno"

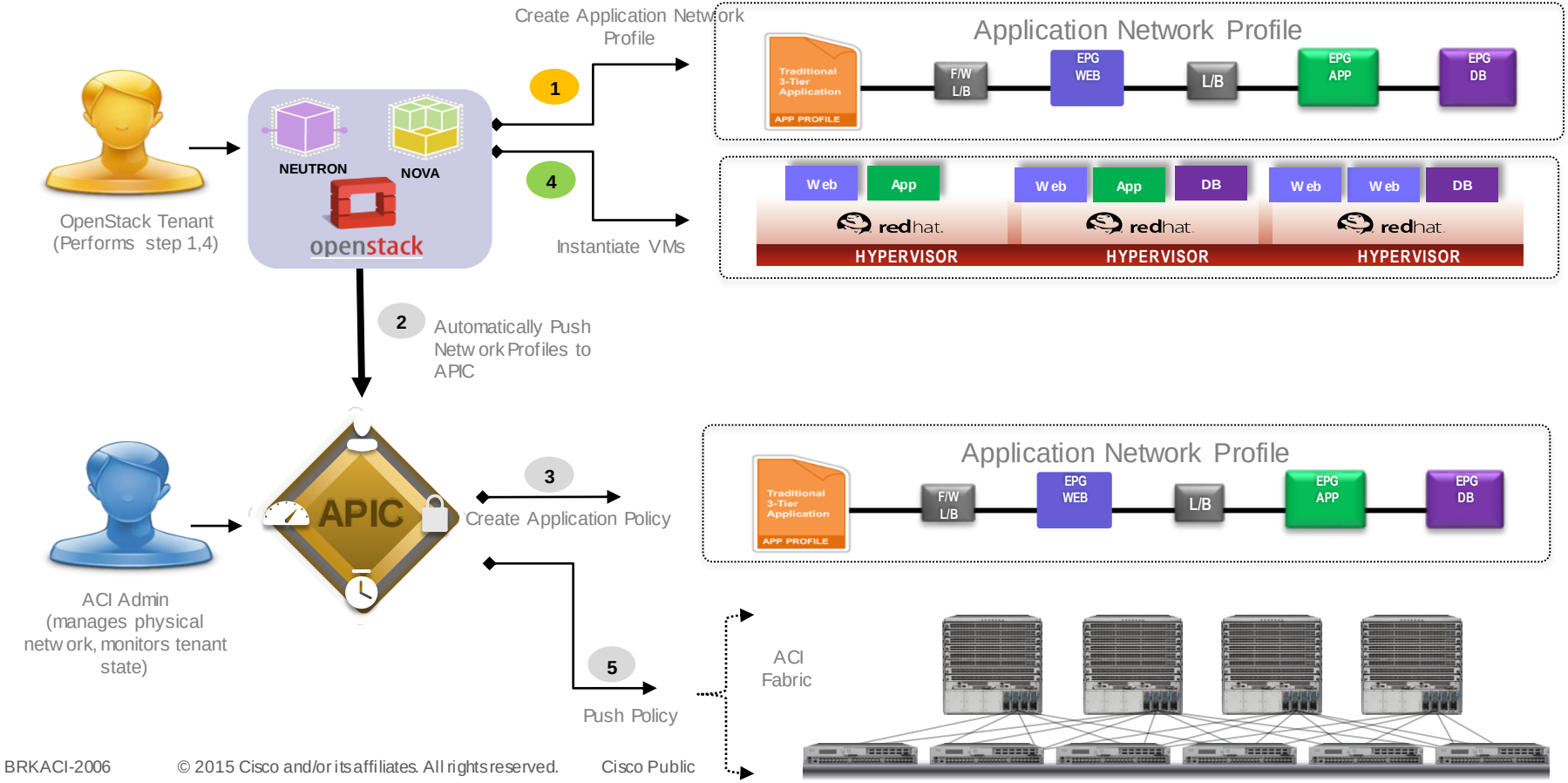
- Messy mapping ACI to current OpenStack component
  - Endpoint groups (ports + security groups)
  - Contracts (security groups + security group rules)
- Goal: Introduce ACI model into OpenStack
- Starting with groups and group-based policies



https://wiki.openstack.org/wiki/GroupBasedPolicy



ACI OpenStack Integration – Phase 2



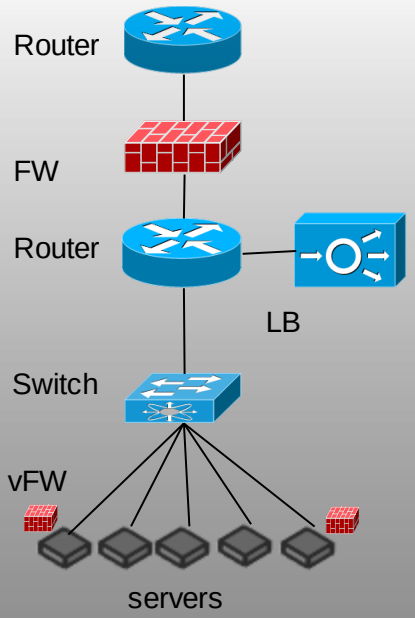
Layer 4-7 Services Integration

Cisco live!

Agenda

- Challenges with Network Service Insertion
- Goals of ACI Services Insertion and Automation
- Key concepts and building blocks
- Services Insertion Configuration Wizard

Challenges with Network Service Insertion



Service Insertion In traditional Networks

- Configure Network to insert Firewall
- Configure firewall network parameters
- Configure firewall rules as required by the application
- Configure Load Balancer Network Parameters
- Configure Router to steer traffic to/from Load Balancer
- Configure Load Balancer as required by the application

Service insertion takes days

Network configuration is time consuming and error prone

Difficult to track configuration on services

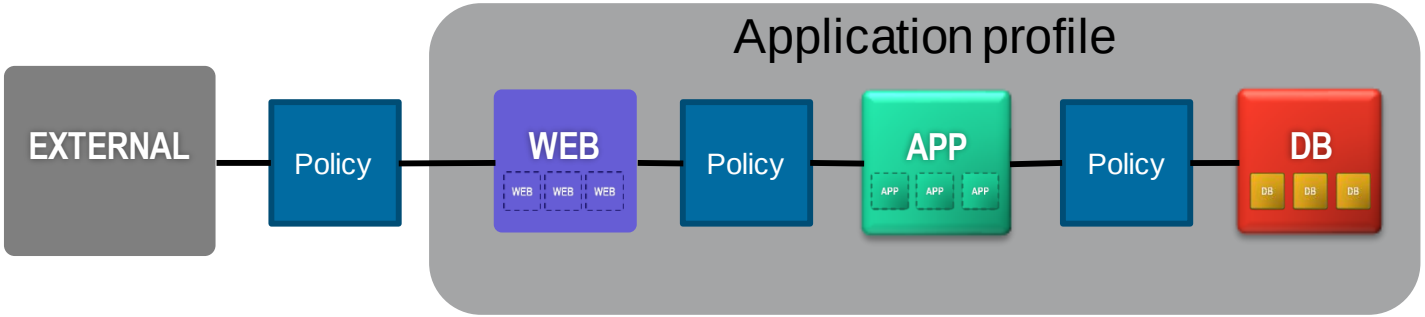
Goals of ACI Service Insertion and Automation

Configure and Manage VLAN allocation for service insertion

Configure the network to redirect traffic through service device

Configure network and service function parameters on service device

APIC Application Profile

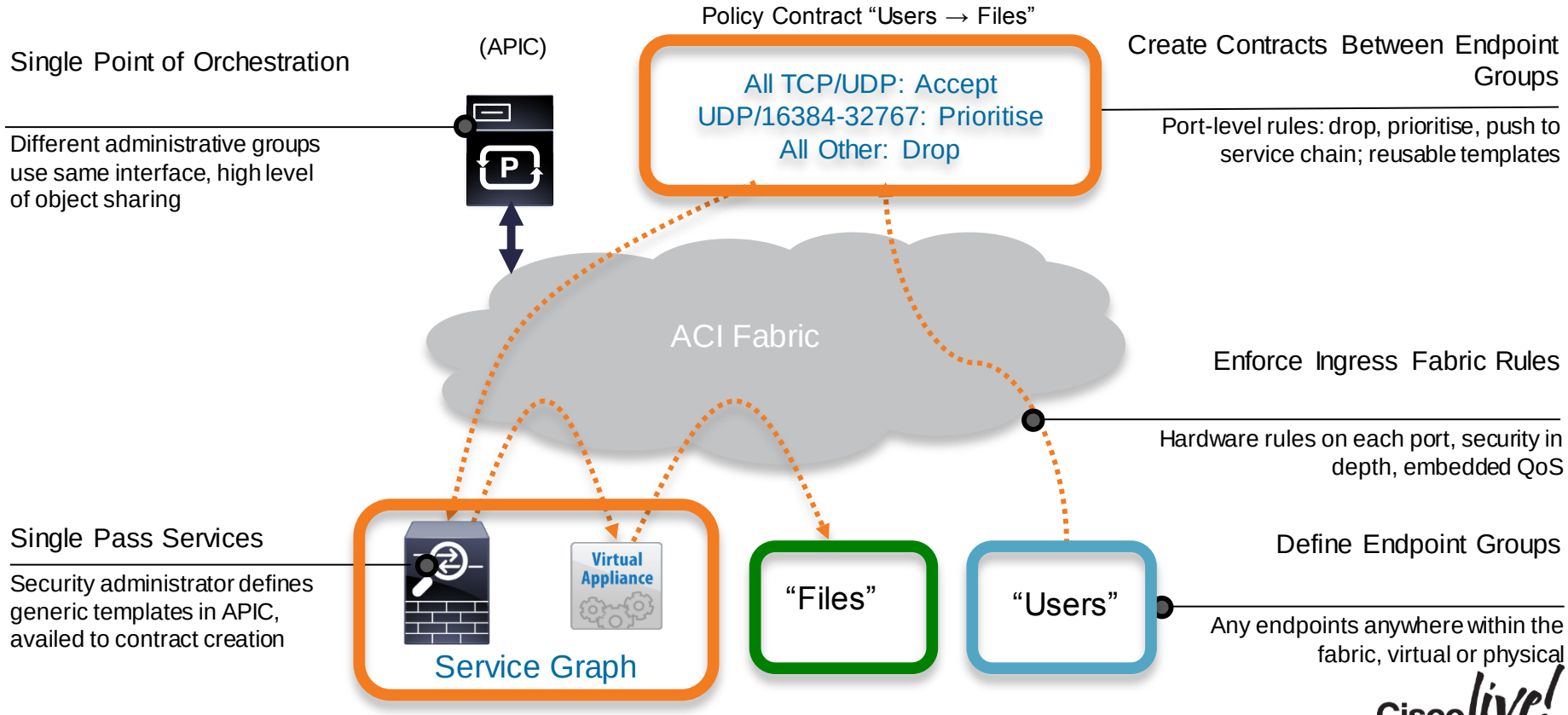


APIC Policy Model

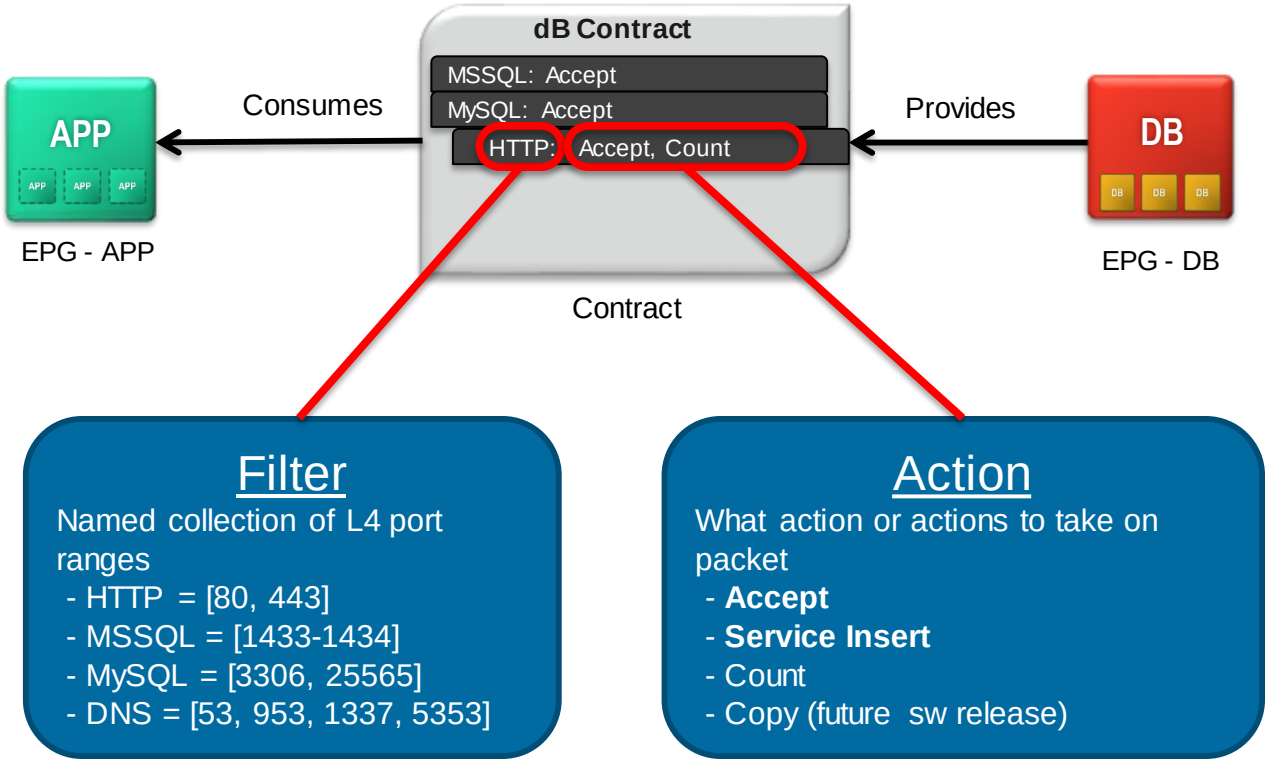
Endpoint Group (EPG): Collection of similar End Points identifying a particular Application Tier. Endpoint could represent VMs, VNICs , IP, DNS name etc

Application Profile: Collection of Endpoint Groups and the policies that define way Endpoint group communicate with each other

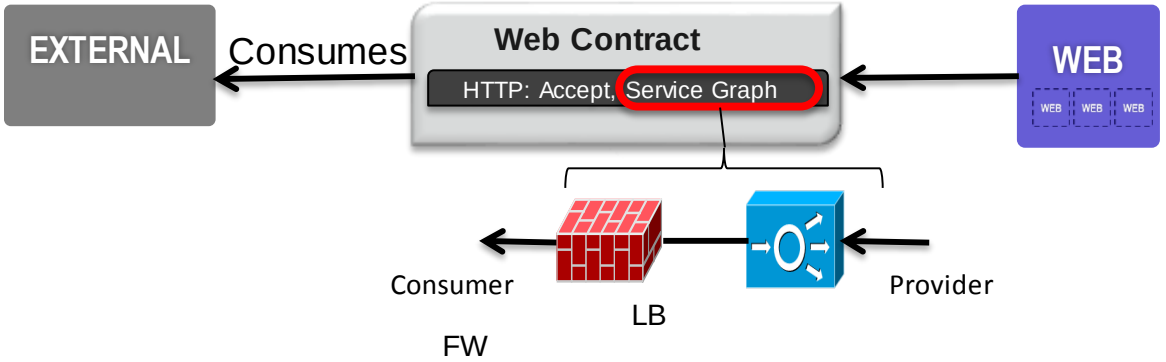
ACI Communication Abstraction



Application Policy



Network Service Insertion



- Contract provides a mechanism to add Network Services through associating a Service Graph
- A Service Graph identifies a set of network service functions required by an application
- APIC configures network service functions on devices like firewall, Load Balancers through a device packages
- A device package can be uploaded on APIC at run time
- Adding new network service support through device package does not require APIC reboot

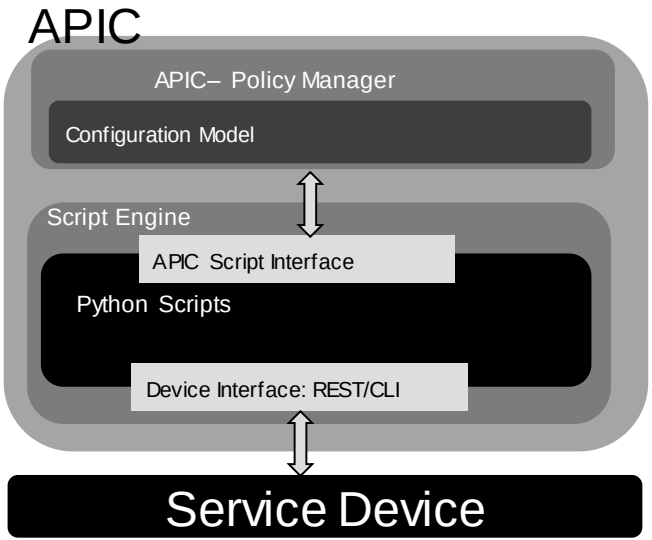
Key Concepts in Service Insertion

- Concrete Device: it represents a service device, e.g. one load balancer, or one firewall
- Logical Device: represents a cluster of 2 devices that operate in active/standby mode for instance.
- Service Graph: defines a sequence of “functions” connected: e.g. a firewall from Checkpoint followed by a load balancing from “F5”.
- Logical Device Context: specifies upon which criteria a specific device in the inventory should be used to render a service graph
- Device Package:
  - defines things such as how to label “connectors” for a function, and how to translate “names” from ACI to the specific device.
  - E.g. a load balancer “function” has predefined connectors called:
    - “external”
    - “internal”
    - “management”.

Service Insertion Architecture

Service functions are added to the APIC through a device package

Device package contains a device model and device python scripts

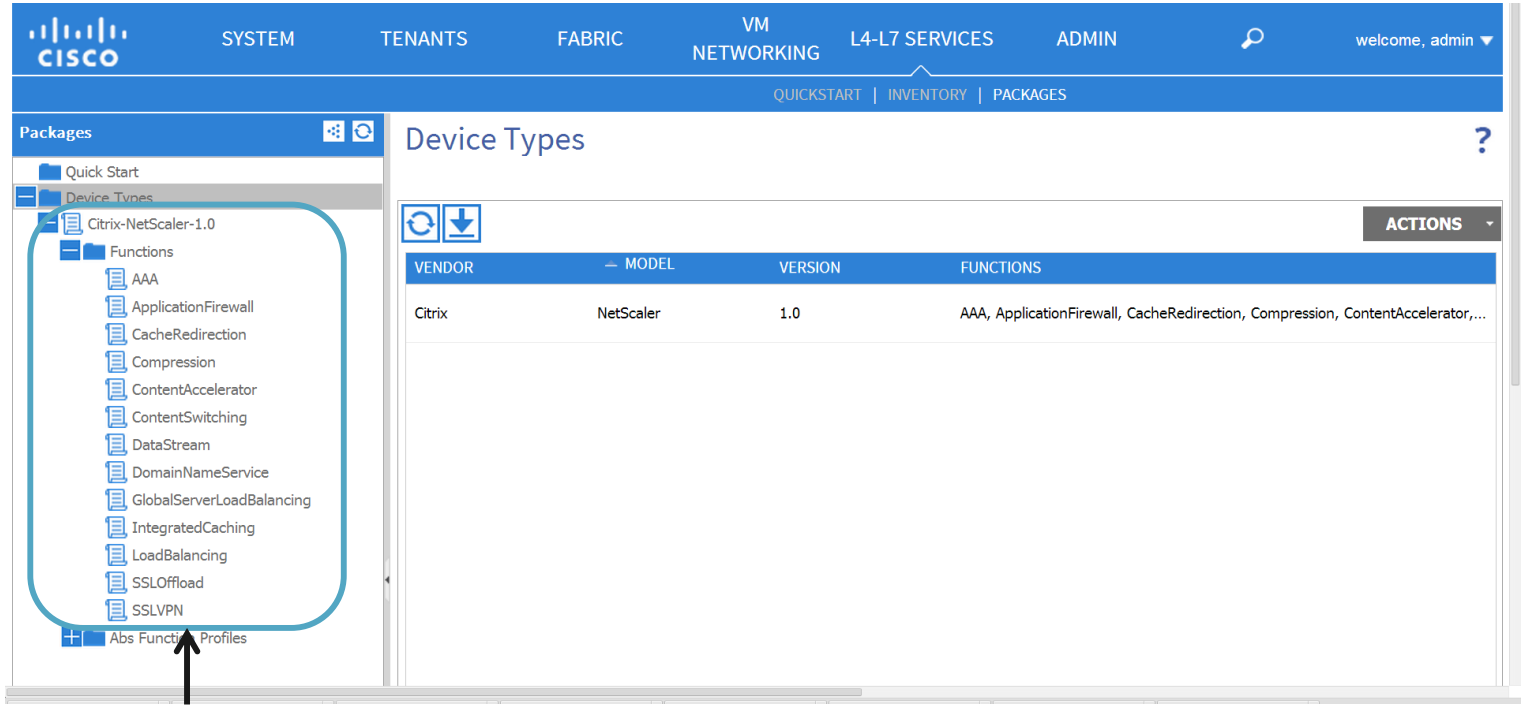


Device Model defines Service Function and Configuration

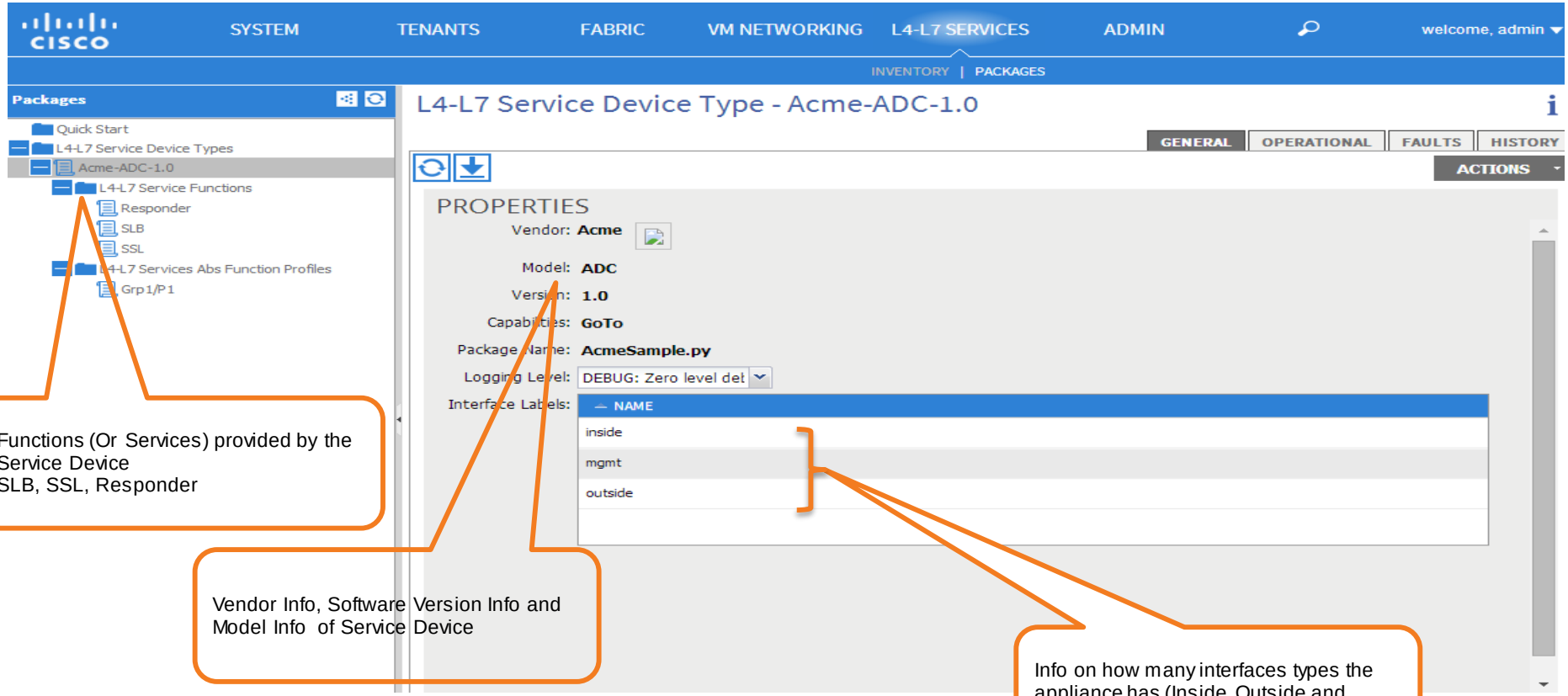
Device scripts translates APIC API callouts to device specific callouts

Script can interface with the device using REST, SSH or any mechanism

Device Package Example



Device Information Extracted Out of Device Package

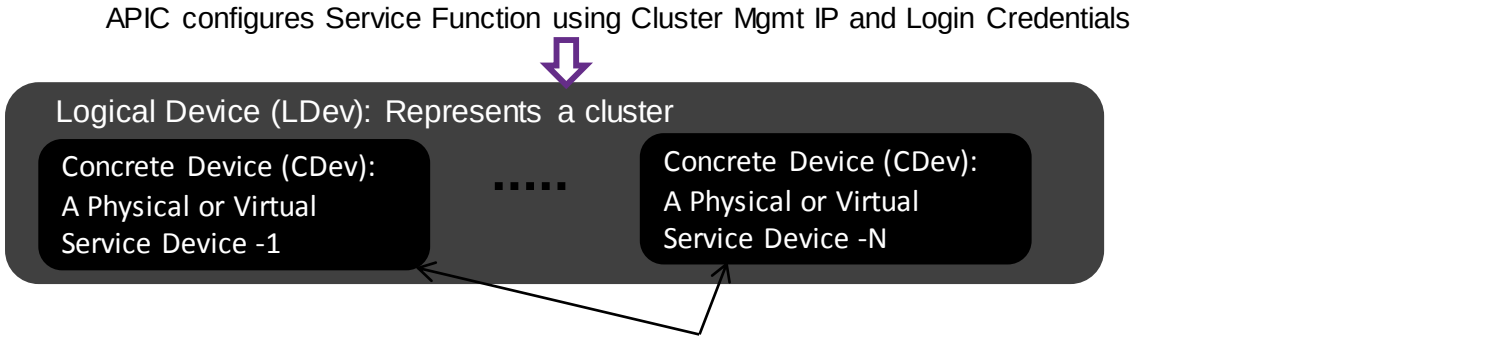


Register Service Devices with APIC

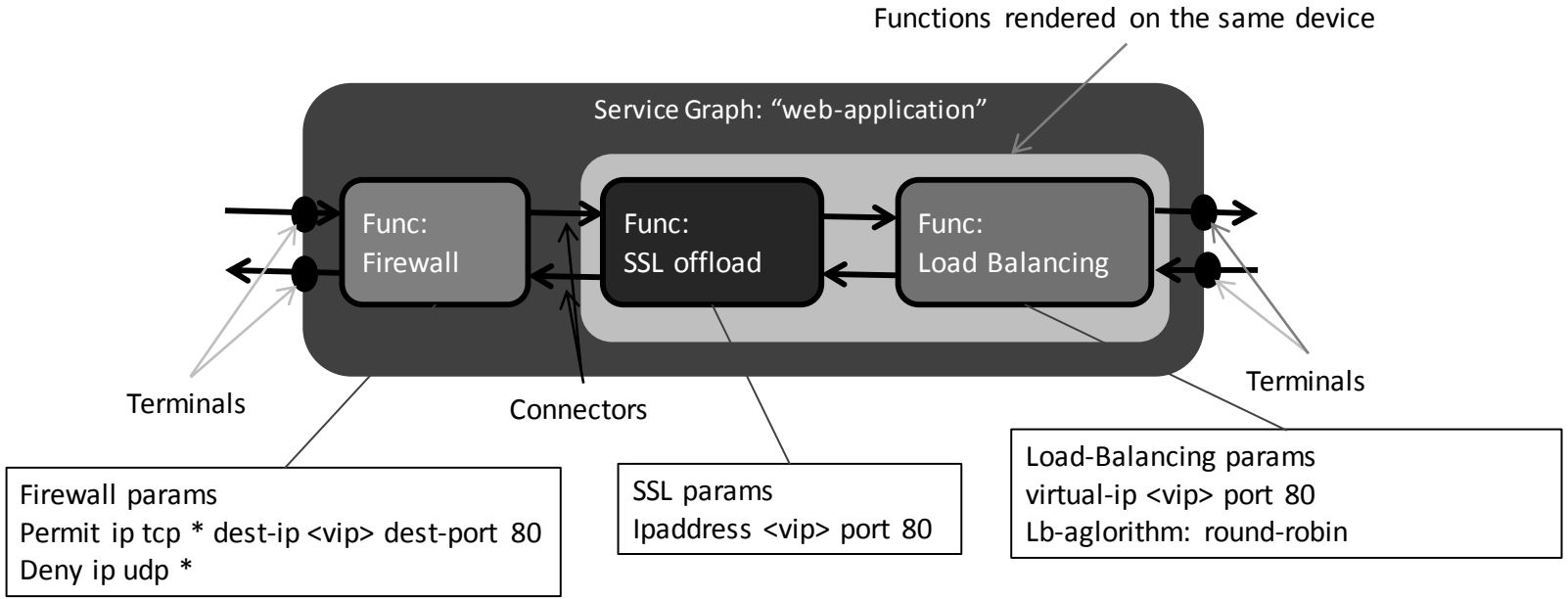
- Configure Management IP address on the device
- Create username/password for APIC to manage the device
- Attach the management interface to appropriate interface/port-group
- Register the device with APIC – Provide IP address and Login credentials

Device Cluster

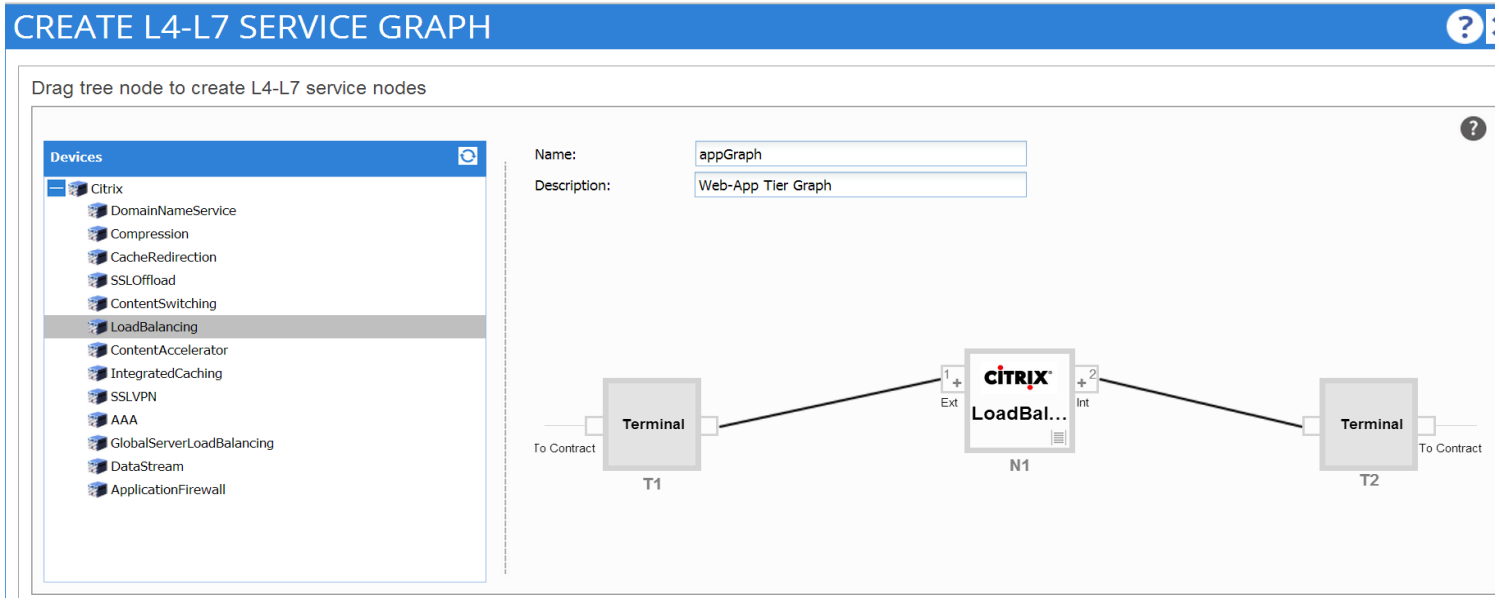
- Devices on APIC are registered as a cluster
- Cluster can contain one or more physical or virtual devices
- Devices within the cluster can be deployed in Active-Active or Active-Standby mode



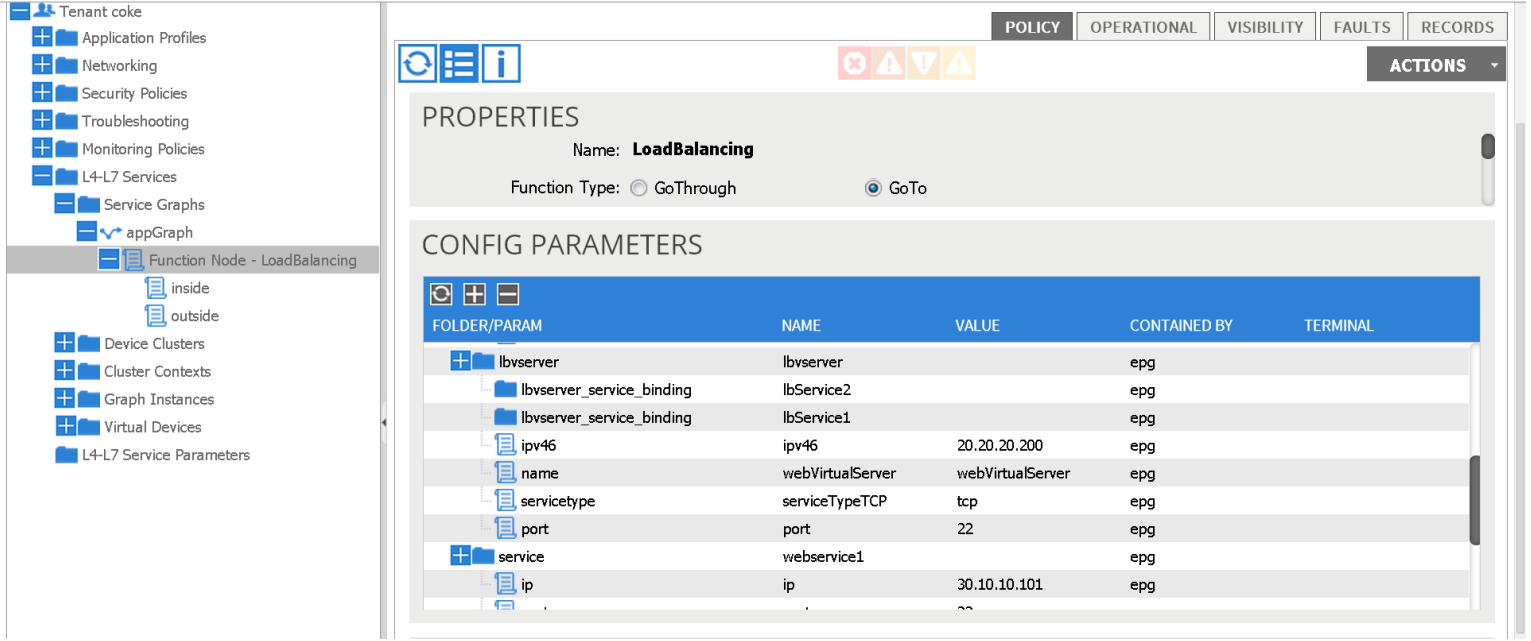
Service Function Graph



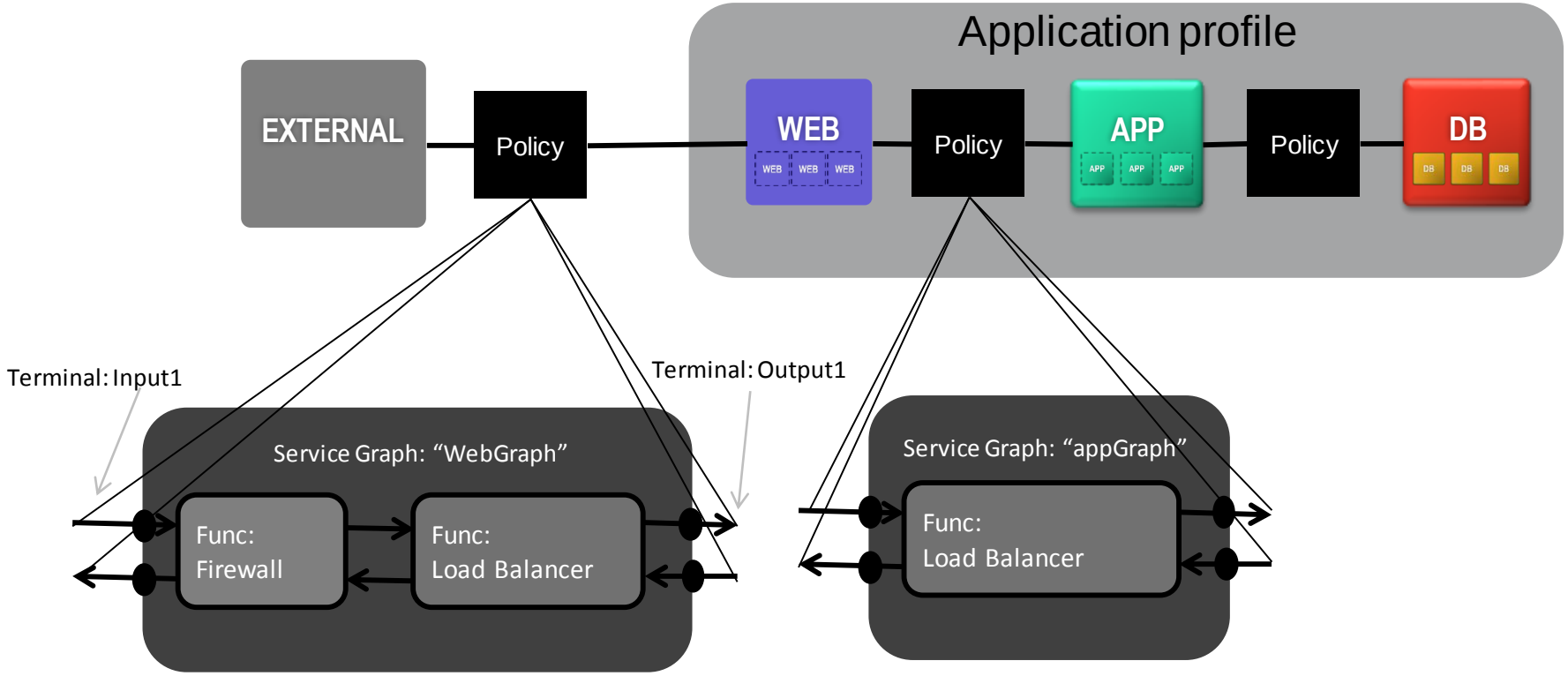
Create Service Graph



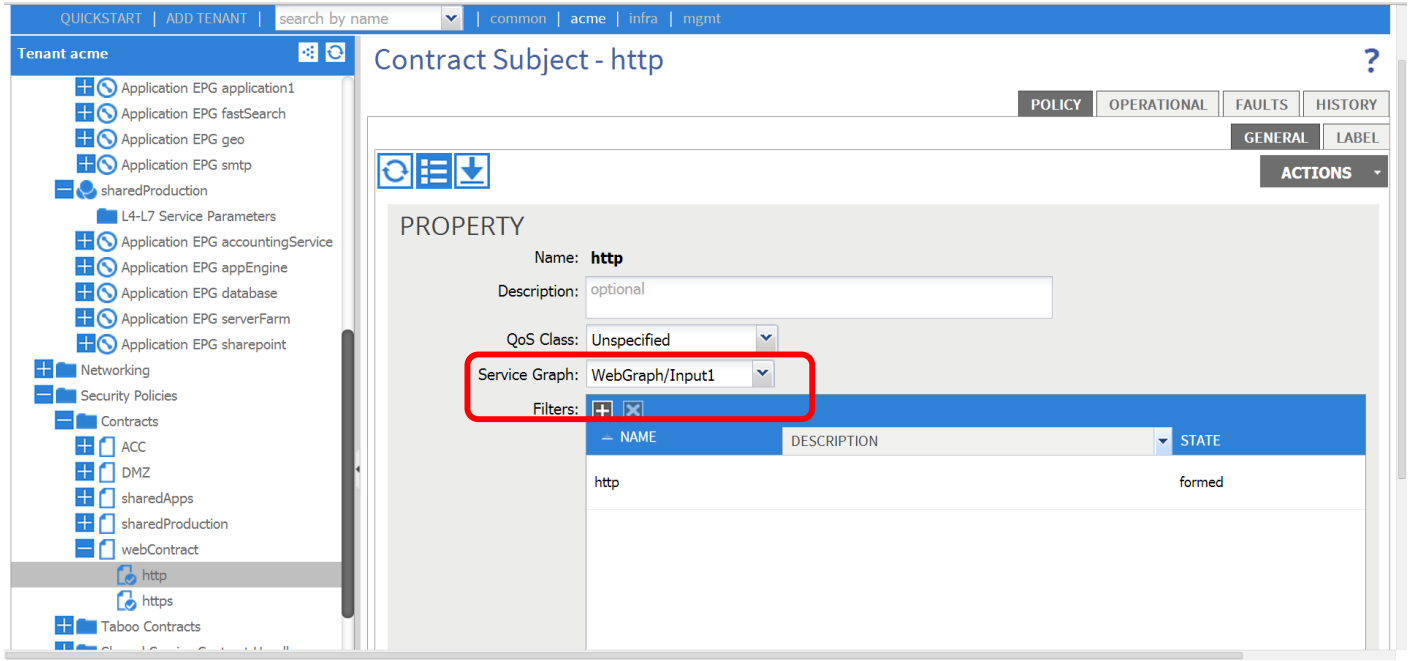
Configure Function Parameters



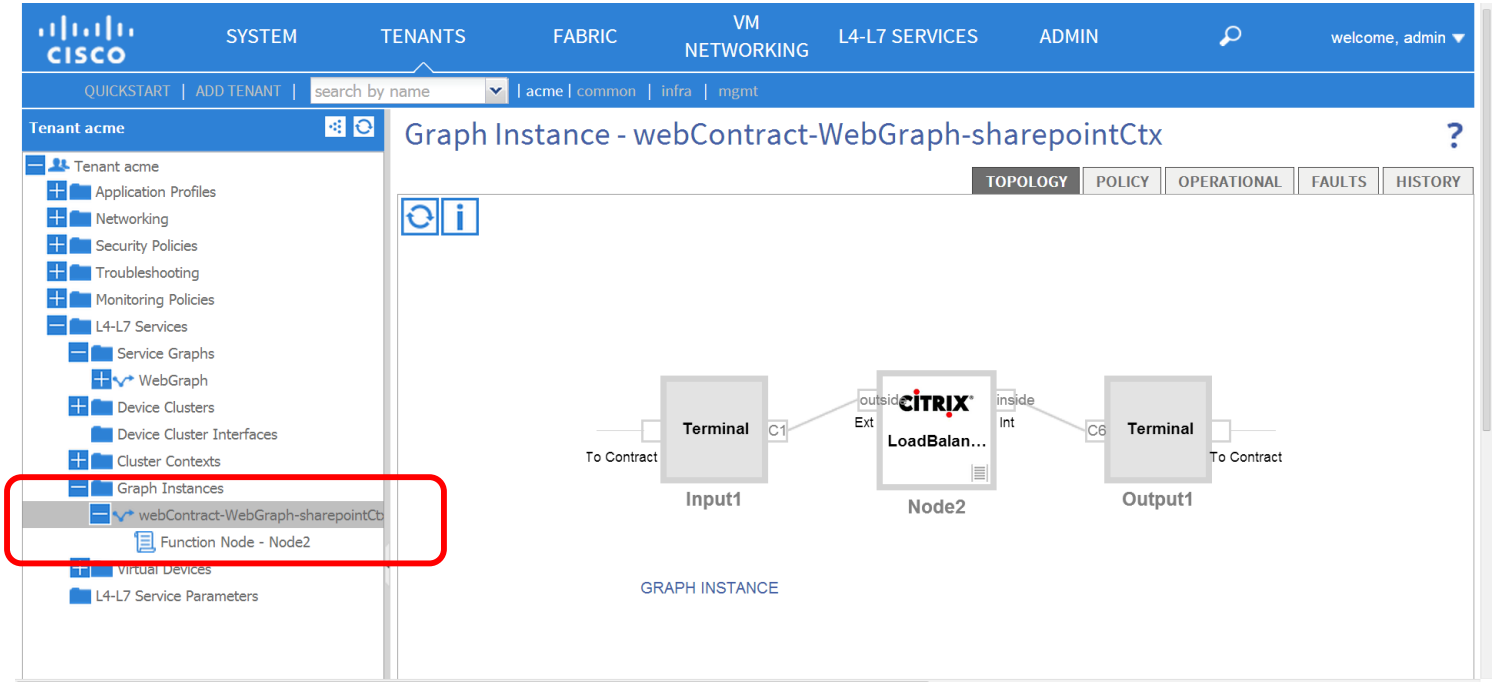
Service Insertion



Associate Graph to a Contract



Example Graph



Services Insertion Configuration Wizard

Three step process and each can be re-used

1. Create L4-L7 Service Devices
2. Create L4-L7 Service Graph Template
3. Apply L4-L7 Service Graph Template to EPGs

Create a L4-7 Service Devices – Single Device

Device Management IP Address and port

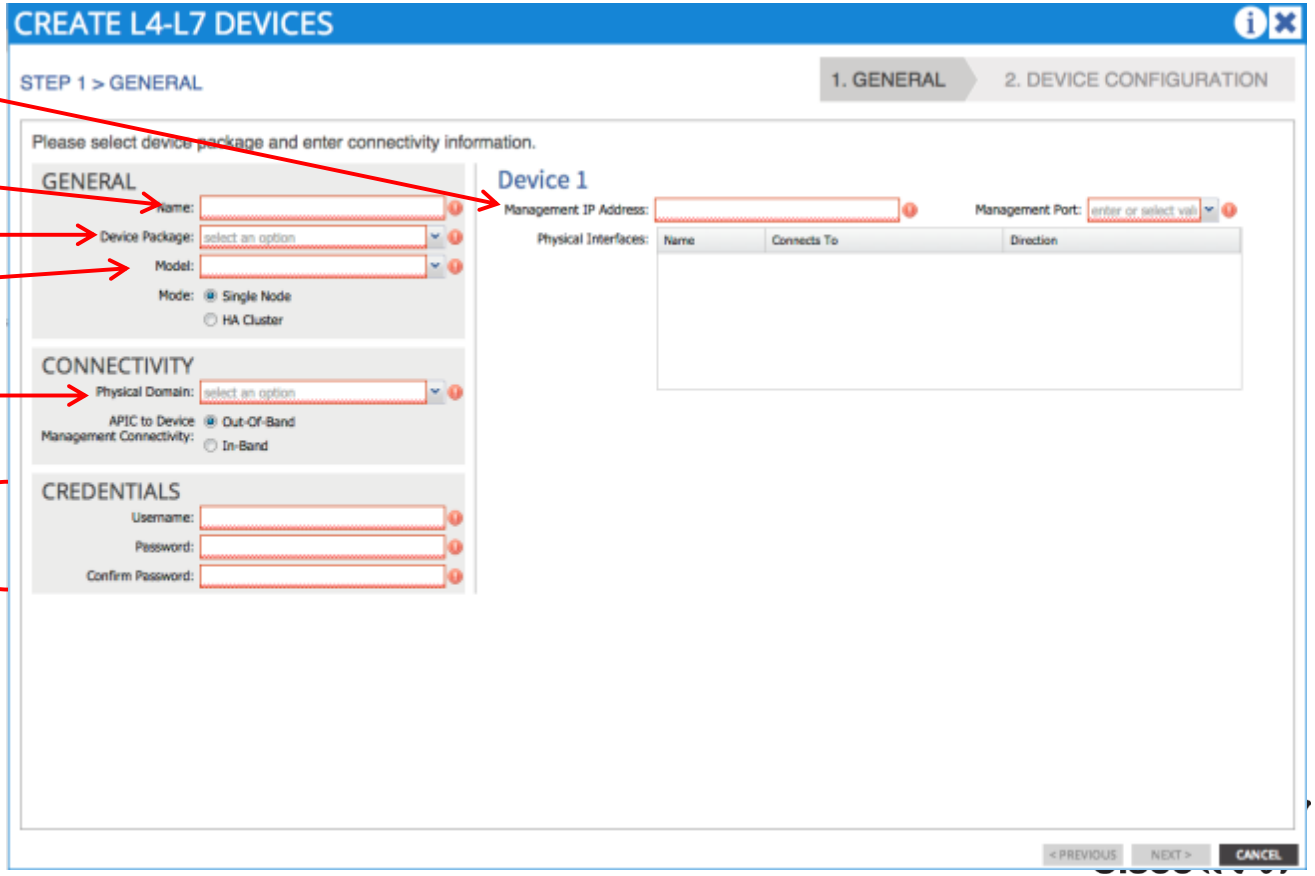
Name of the device

Specify Device Package to manage this Cluster

Model of the device

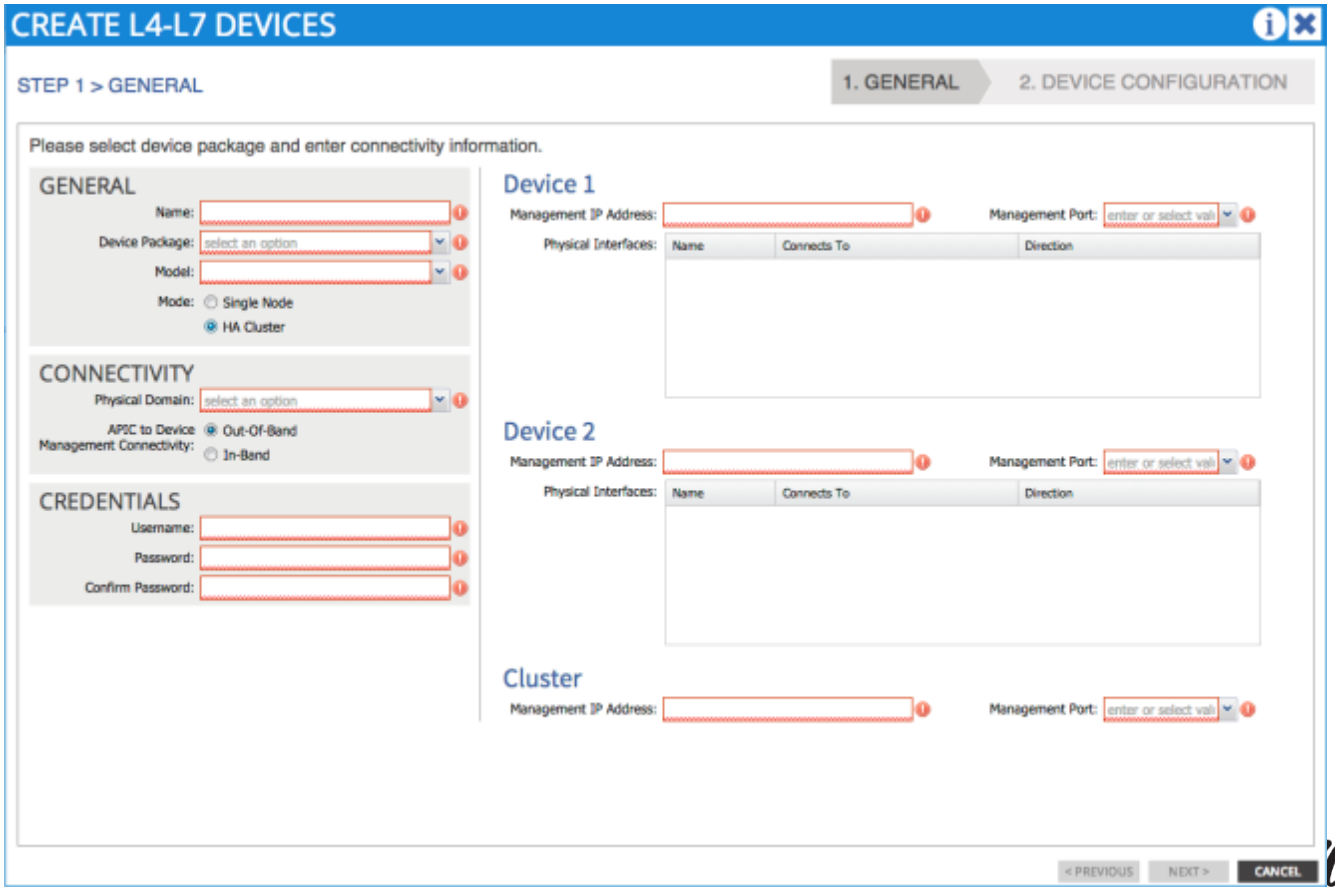
Policy domain

Login Credentials to manage the device and connectivity information



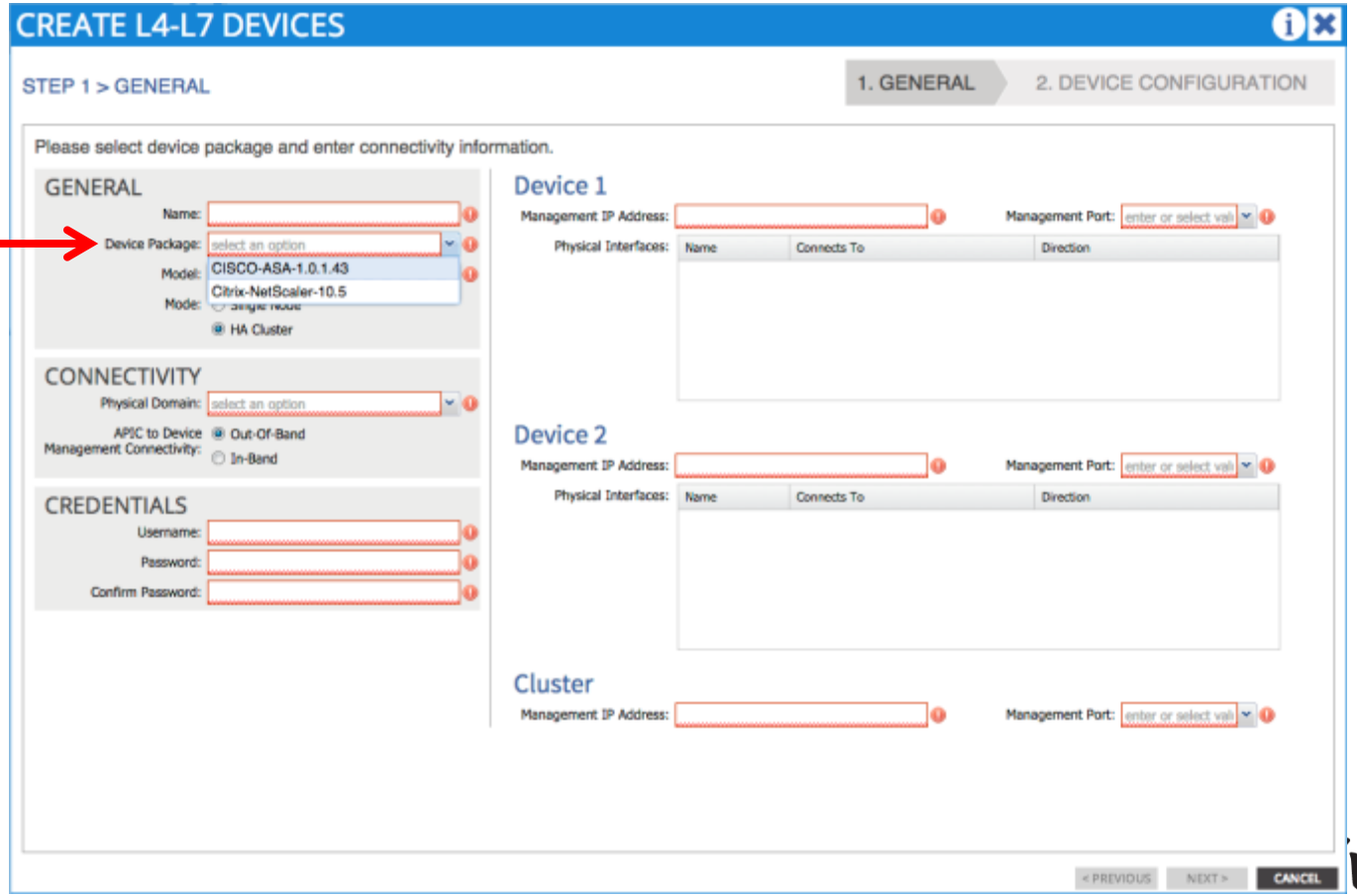
Create a L4-7 Service Devices - HA

This shows how Wizard will look if you select HA Cluster



Create a L4-7 Service Devices – Device Package

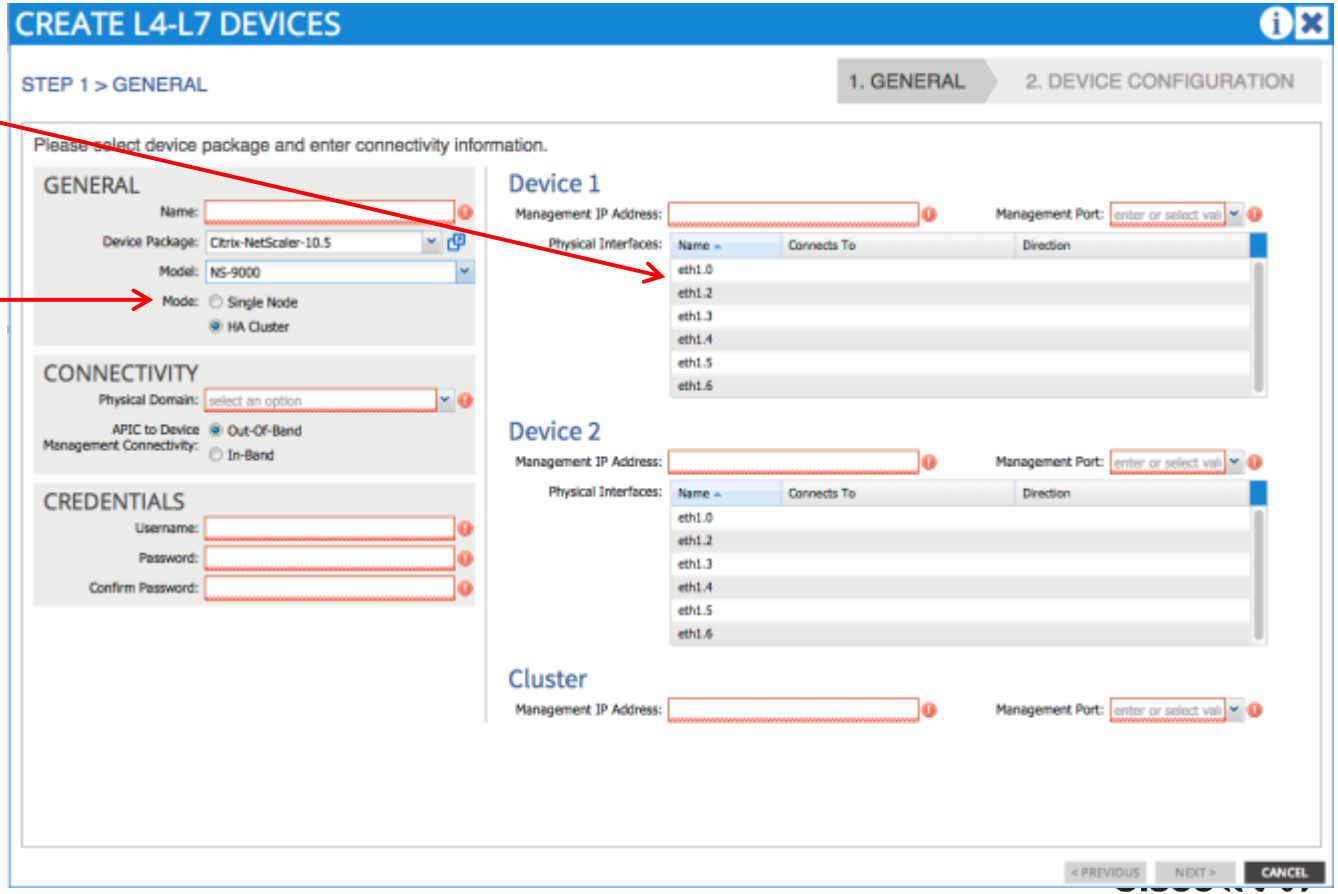
List of device package that APIC has will be shown here



Create a L4-7 Service Devices – Model (Citrix)

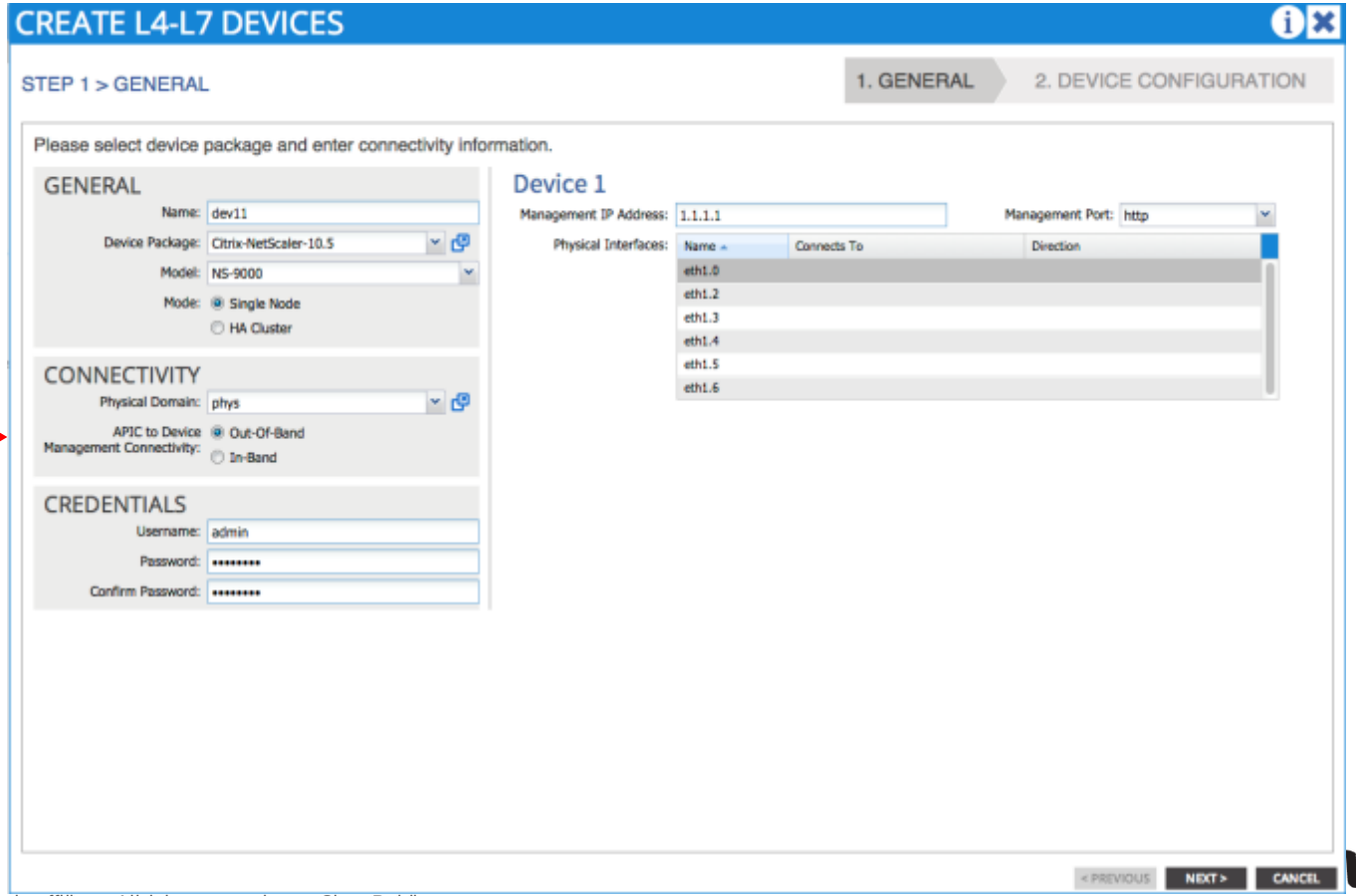
Associated interfaces on the device to interface labels

Single device or cluster / HA



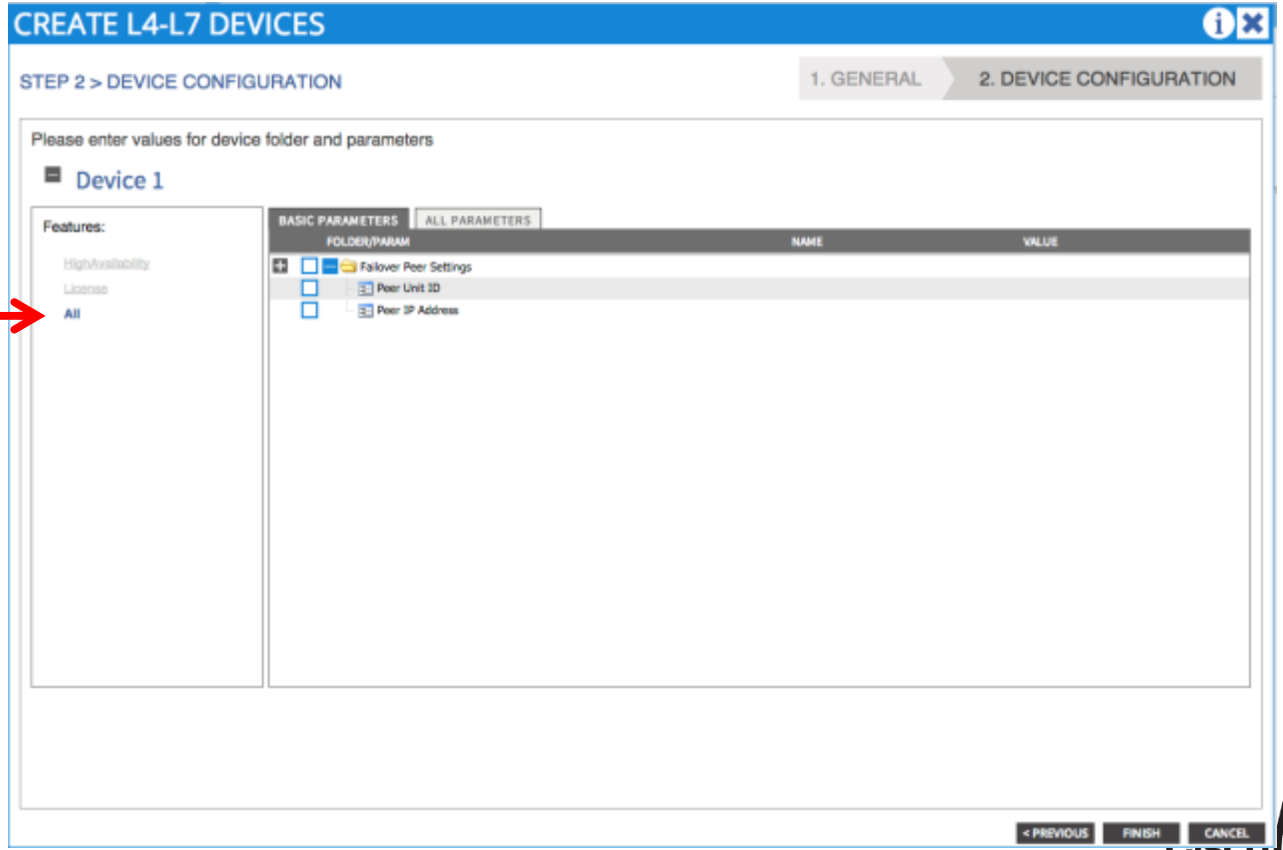
Create a L4-7 Service Devices – Connectivity (Citrix)

Management connectivity to the device



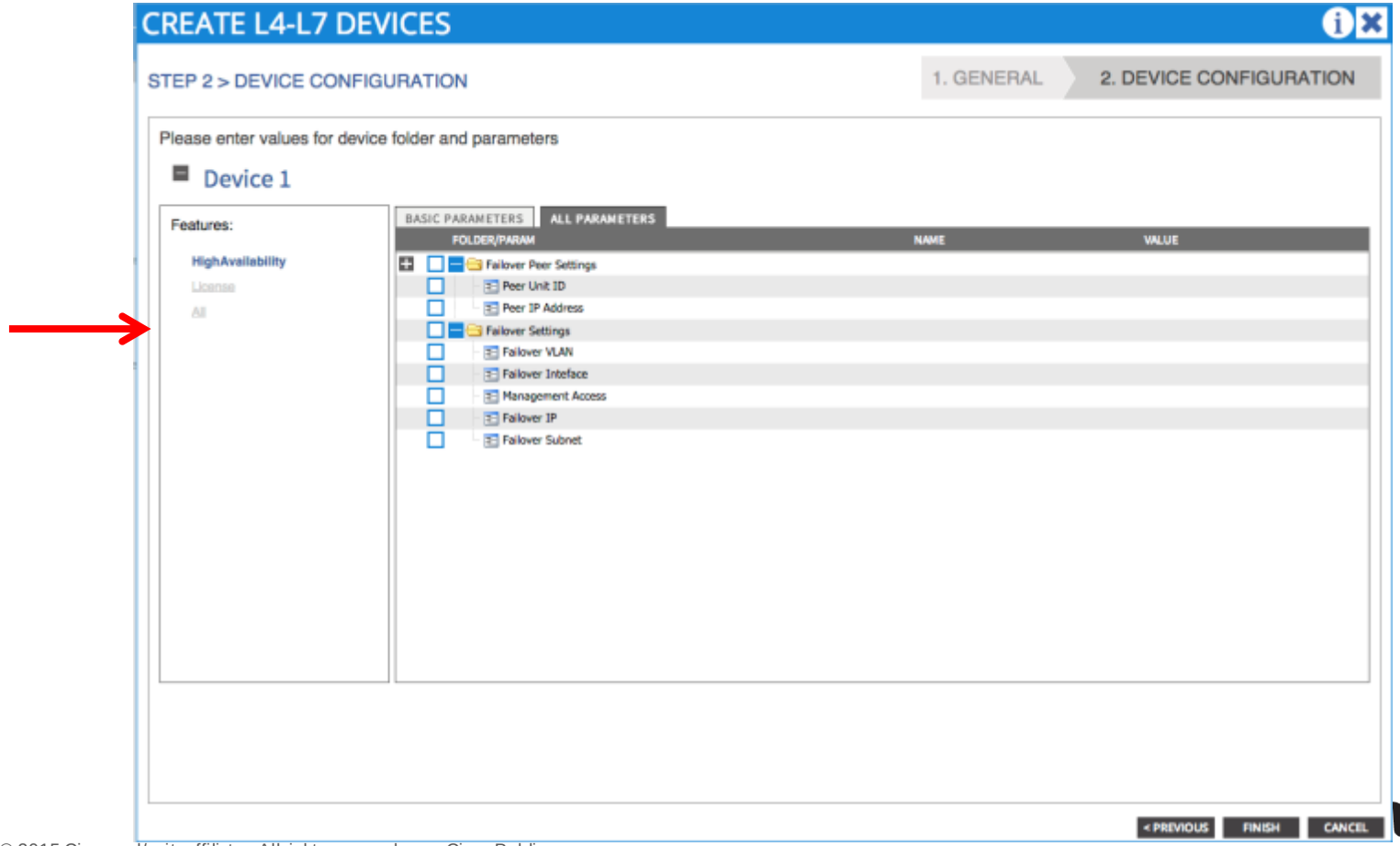
Create a L4-7 Service Devices – Connectivity (Citrix)

Device Parameter that is required.



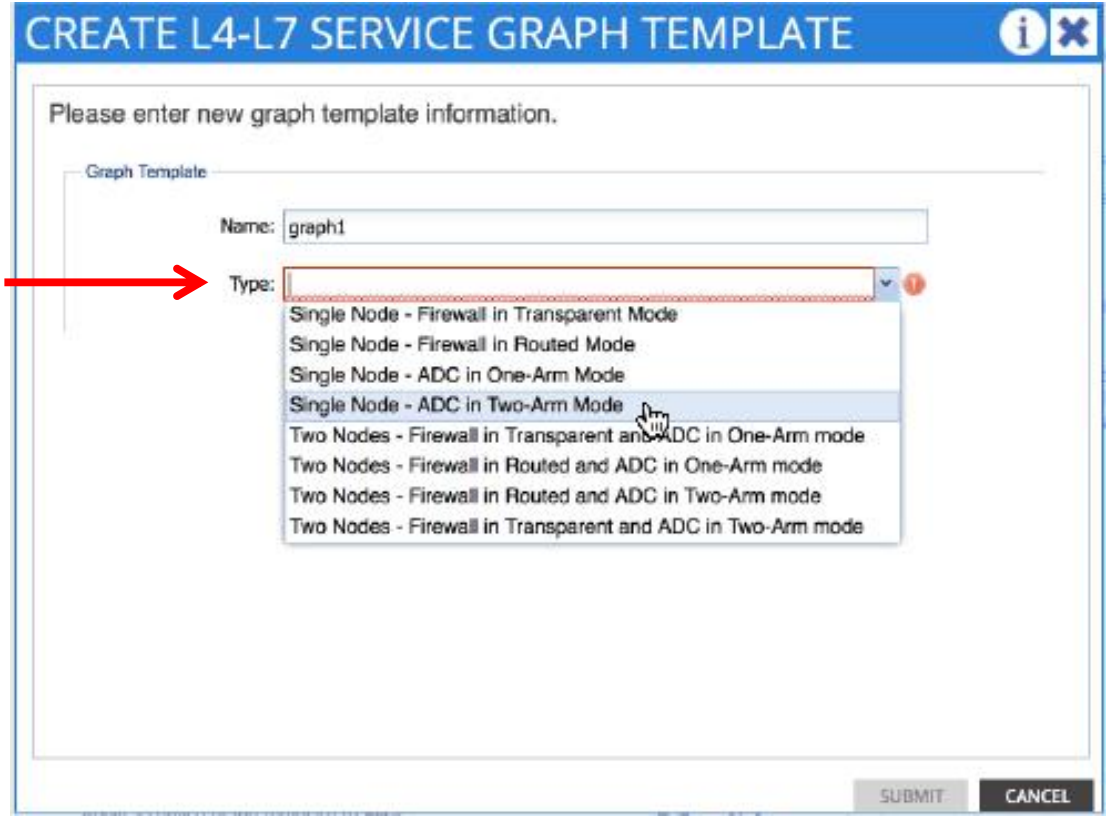
Create a L4-7 Service Devices – Connectivity (Citrix)

Shows all the parameters



Create a L4-7 Service Graph Template

Templates gives you option to choose simple Service Graph based on your requirement



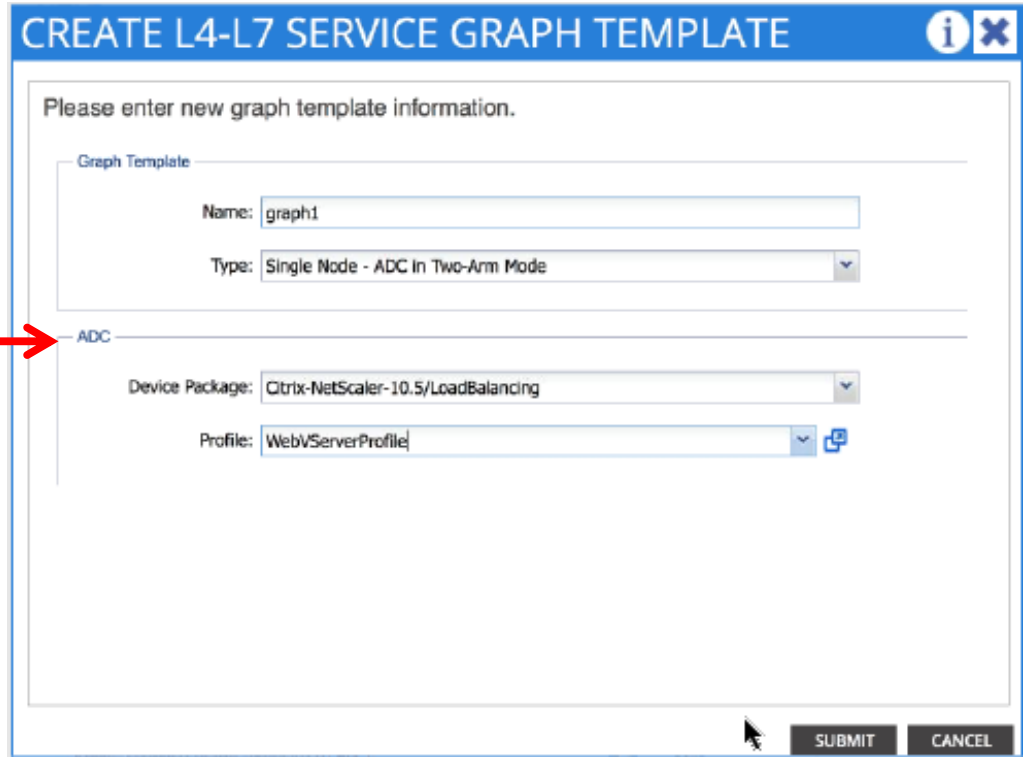
Create a L4-7 Service Graph Template

Single Node ADC

Device Package gives you an option that you want to use for the particular Services Graph

Profile will give the service graph all the parameters that is needed. E.g. SSL

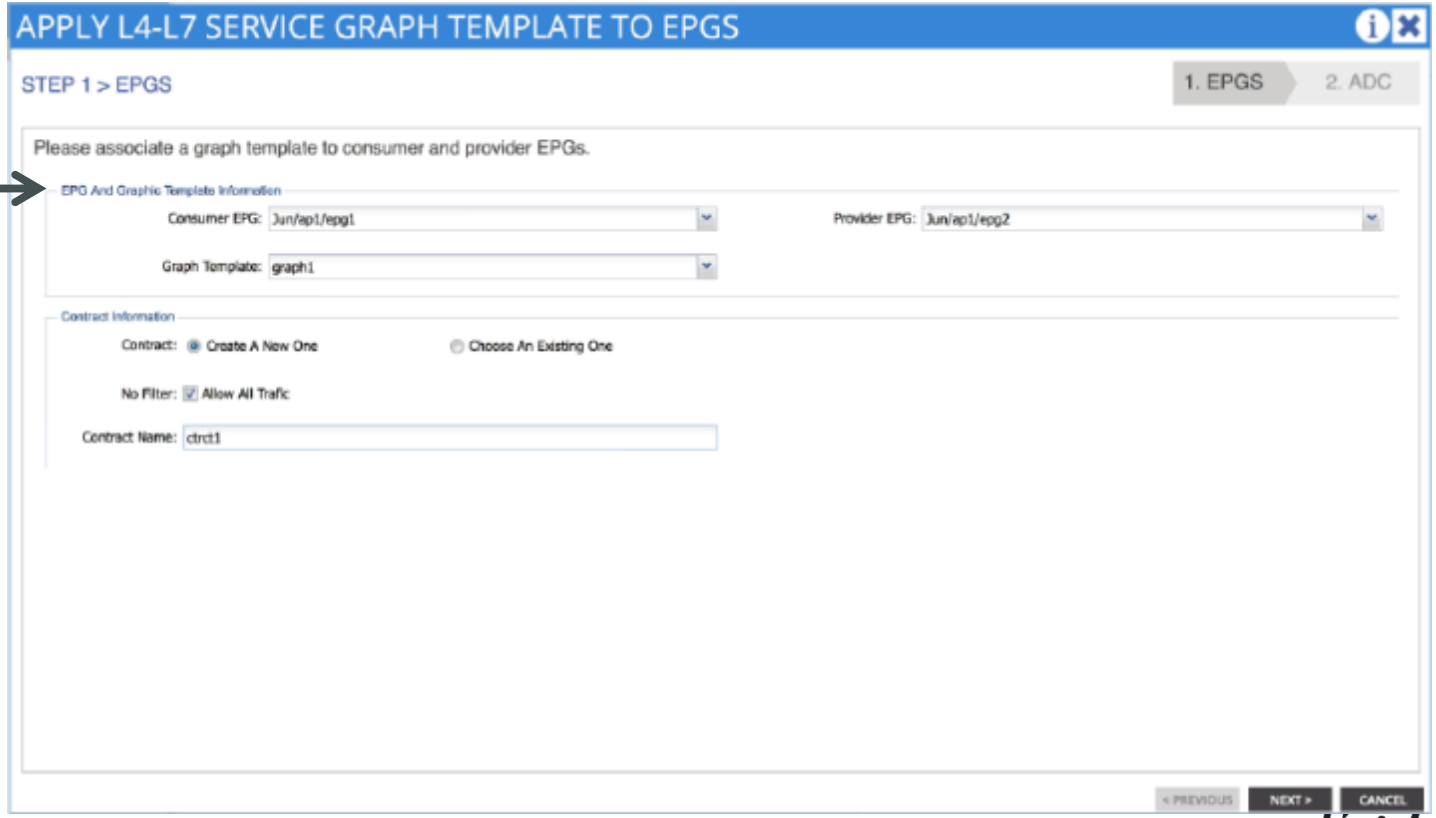
Users can also customise the profile. You can click on profile to see what parameters are available.



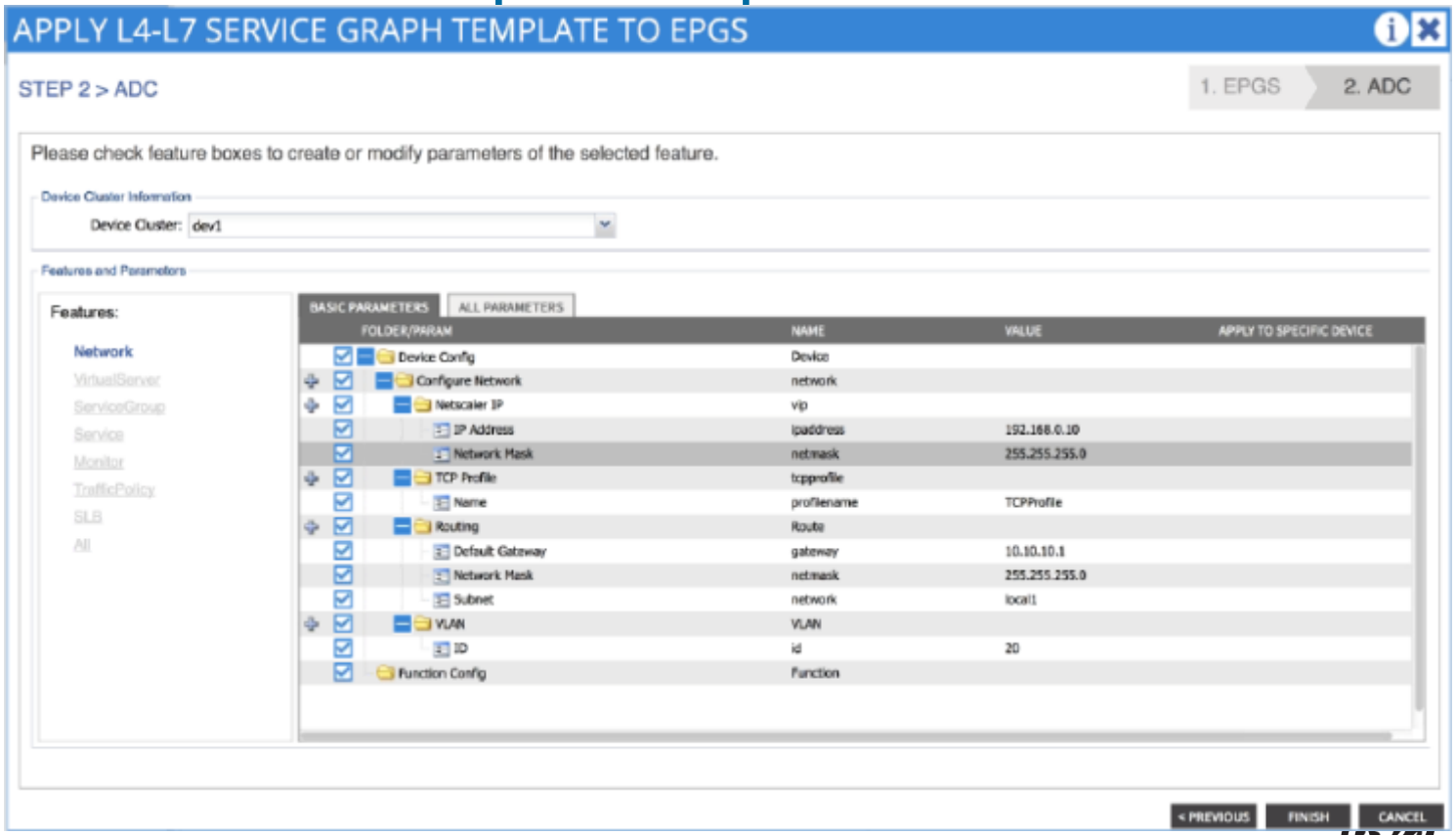
Apply L4-L7 Service Graph Template to EPGs

EPG and Service Graph Template

If you uncheck “Allow All Traffic” i.e. IP Any any or you can create your own specific filter entries



Apply L4-L7 Service Graph Template to EPGs




Q & A

Complete Your Online Session Evaluation

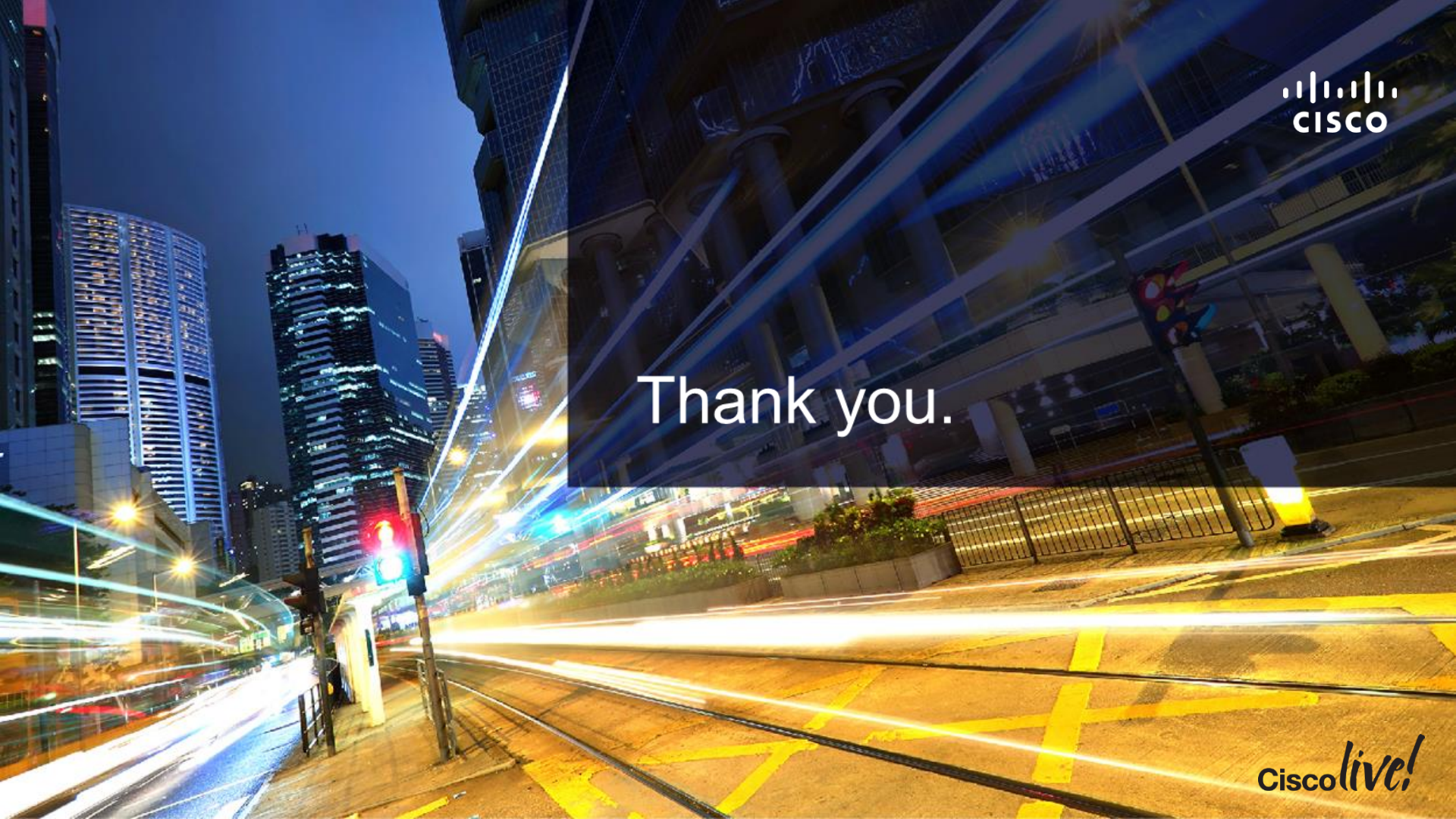
Give us your feedback and receive a Cisco Live 2015 T-Shirt!

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