Cisco ACI - OpenStack Benefits

Meir Roth
Feb 2017

Cisco Nexus Portfolio - Momentum

17,100+
36+% Growth of N9K & N3K Global Customers

9,500+
ACI Ready Customers

2,700+
ACI Customers

65
Ecosystem Partners

Tetration
Analytics Launch
Strong Interest & Uptake

CloudCenter
Strong Bookings Since April Acquisition

Sample List of Public ACI Production Customers

Market Traction Across All Geographies and Market Segments

Cisco architectural approach to SDN with Automation and Programmability

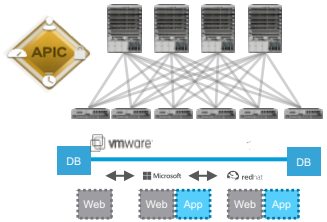
Choice in Automation and Programmability

Application Centric

Turnkey integrated solution with security, centralized management, compliance and scale

Automated application centric-policy model with embedded security

Broad and deep ecosystem



Programmable Fabric

BGP EVPN standard-based

3rd party controller support

Nexus Fabric Manager / DCNM 10 for automation and management across N2K-N9K

Programmable Network

Application Optimized Networks w/Segment Routing

Modern NX-OS with NX-API REST/YANG/OpenConfig

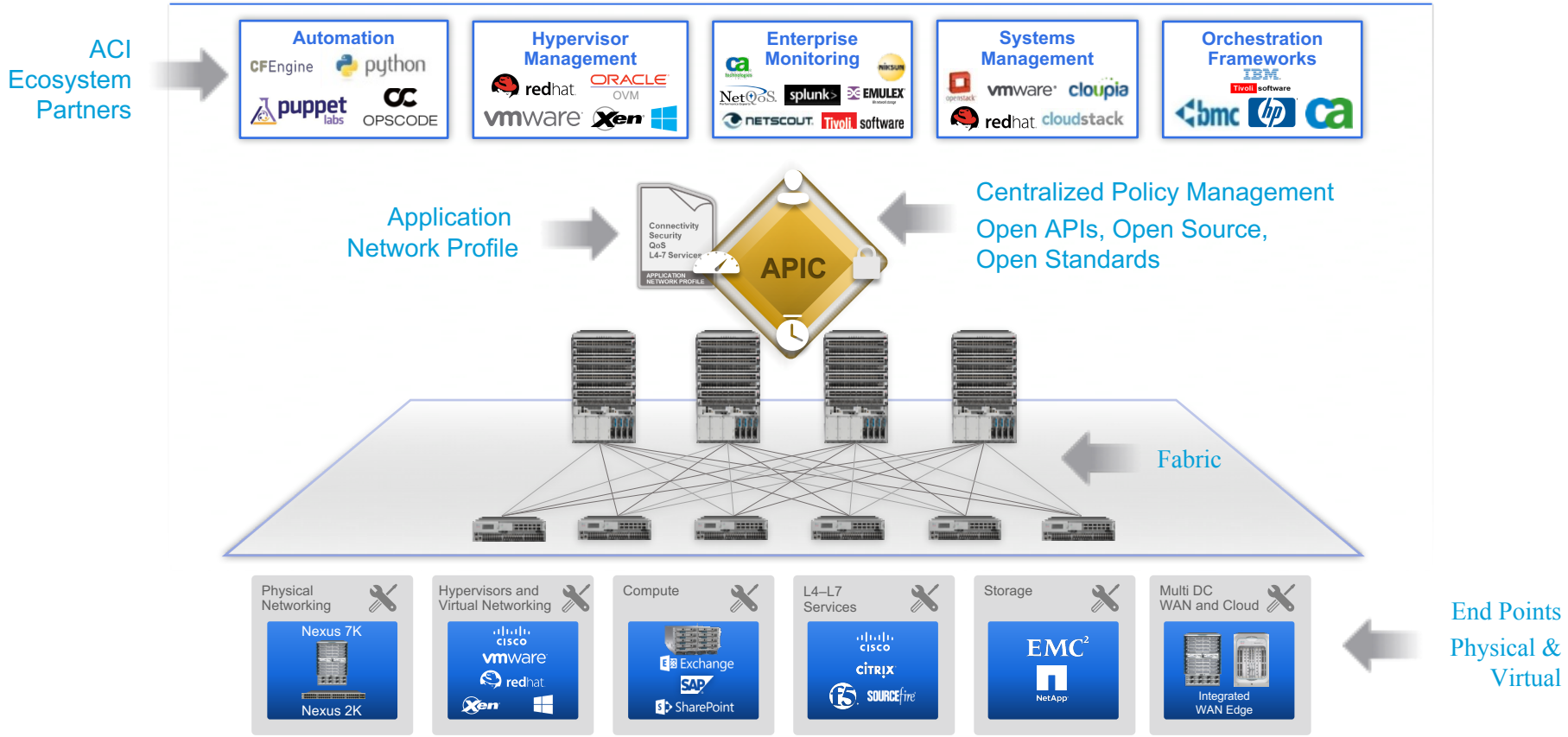
DevOps toolset used for Network Mgmt (Puppet, Chef, Ansible etc.)

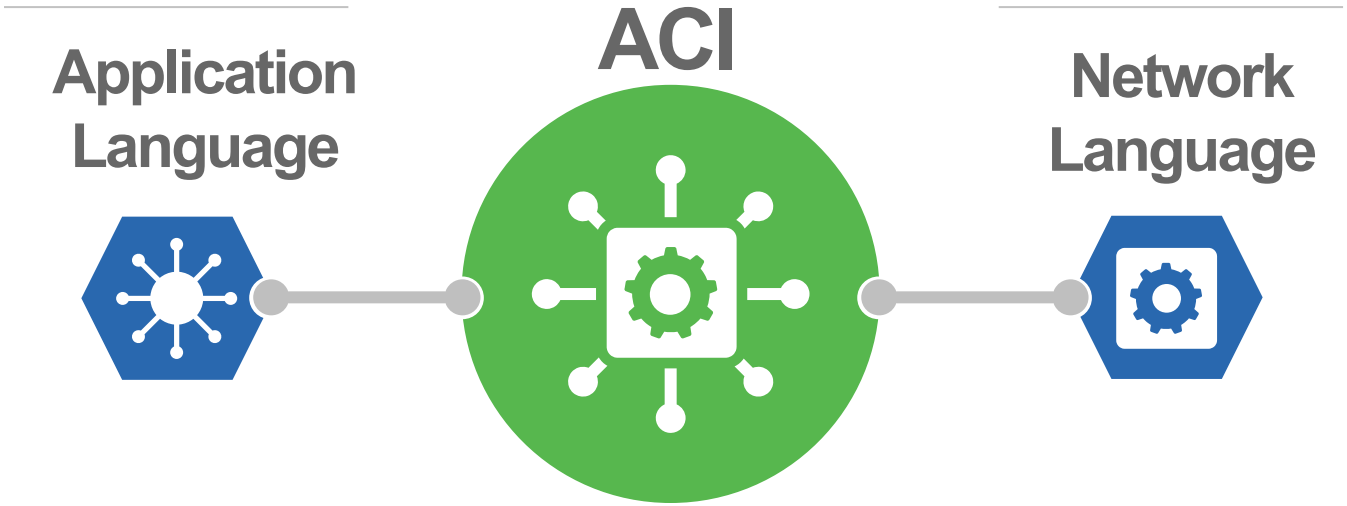
Automation, API's, Controllers and Tool-chains

What is ACI?

At a high level, ACI is network virtualization via policies that are defined around the requirements of an application.

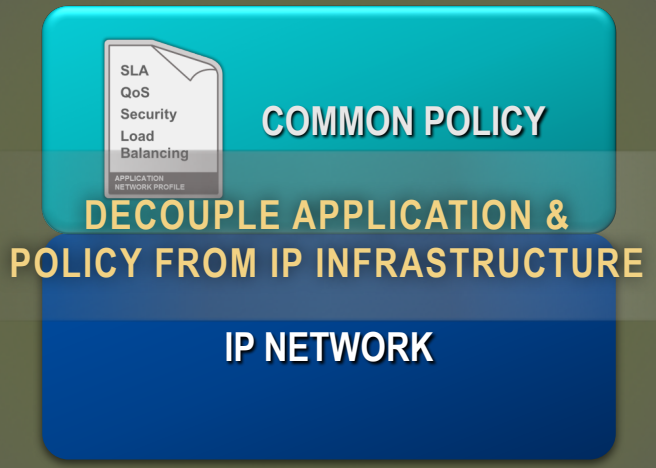
Application Centric Infrastructure Components



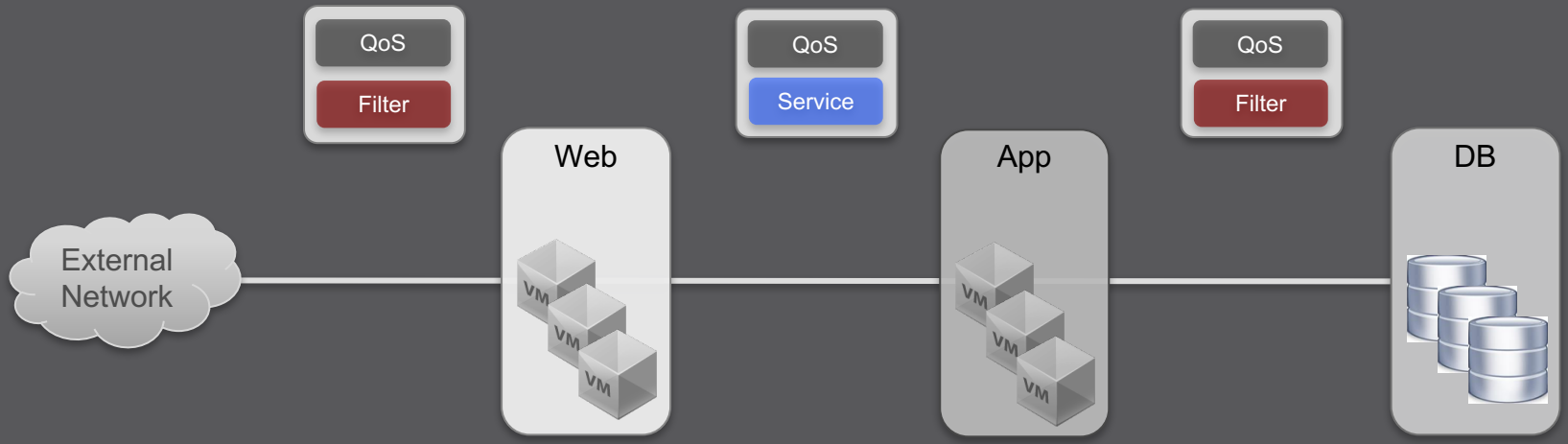


Push configurations automatically to the entire network

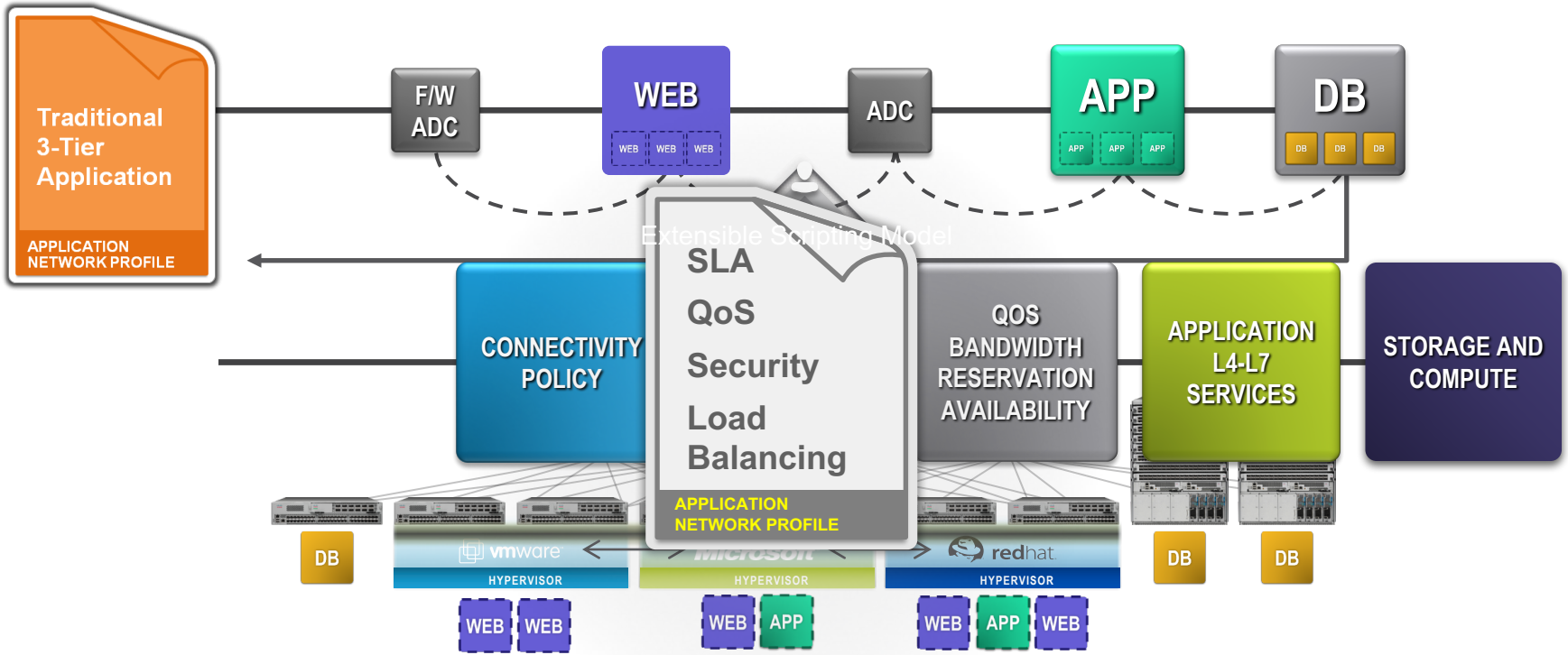
SIMPLIFICATION

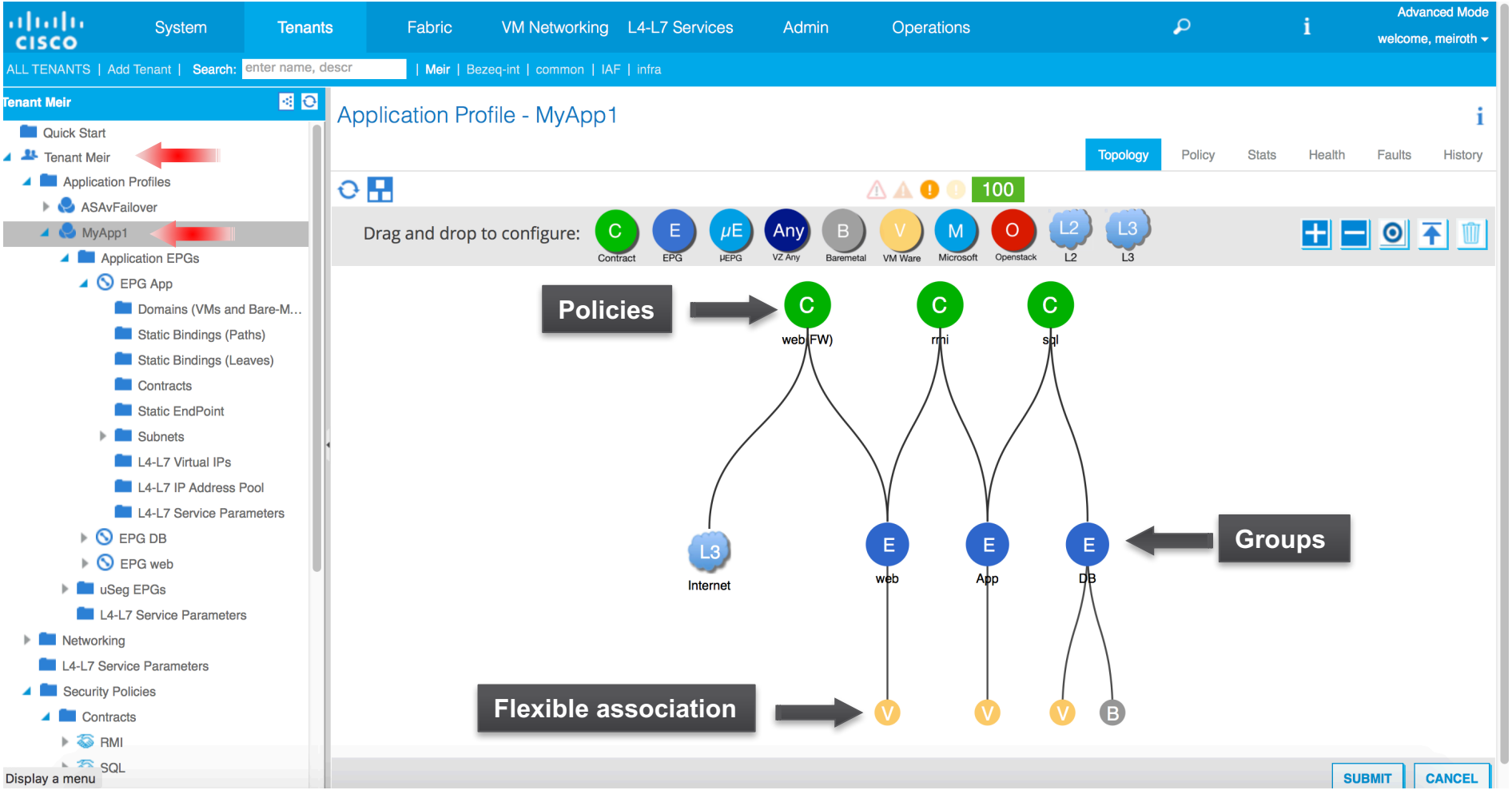


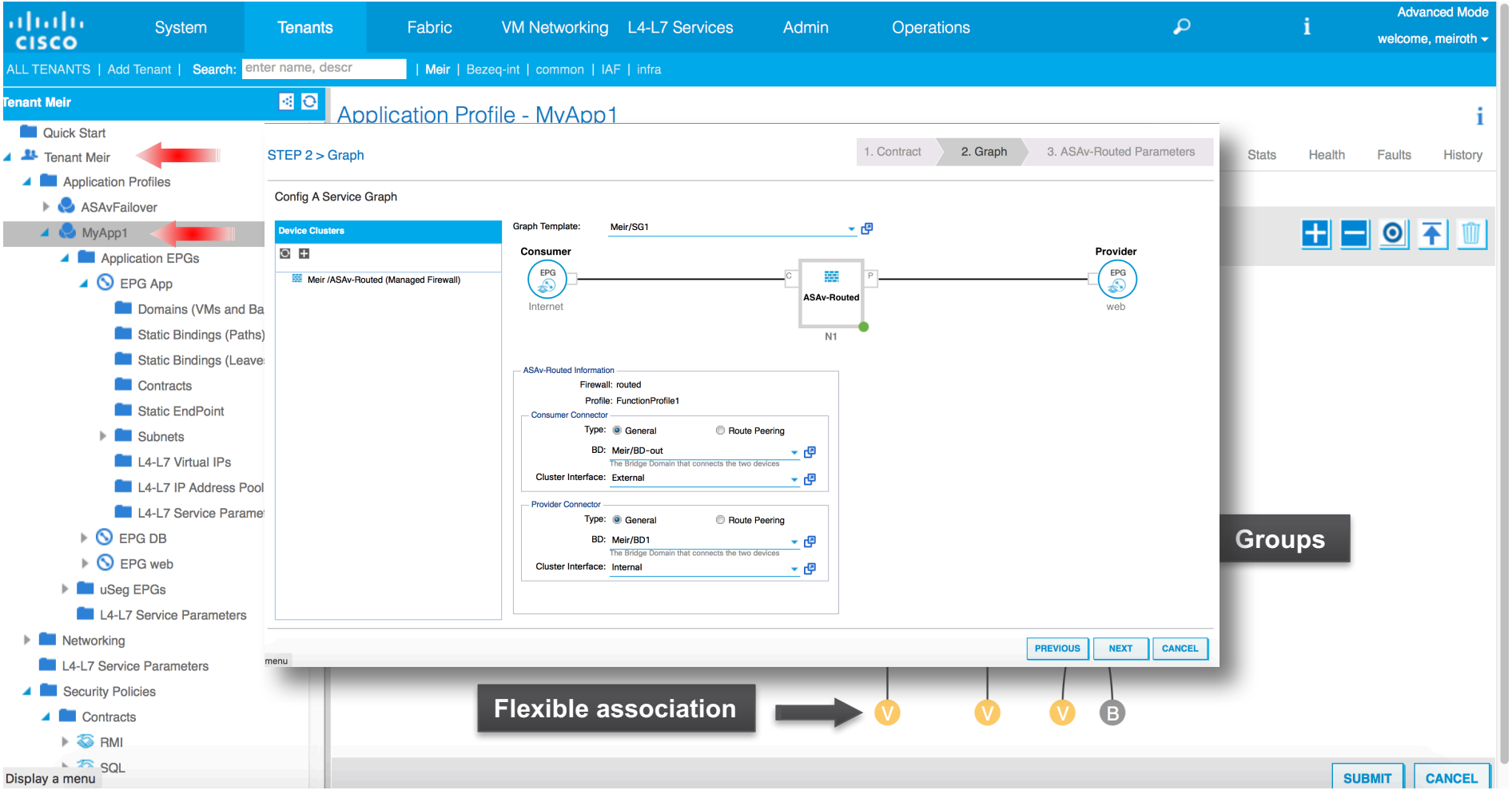
ACI uses a policy based approach that focuses on the application.



AGILITY: ANY APPLICATION, ANYWHERE—PHYSICAL AND VIRTUAL
COMMON APPLICATION NETWORK PROFILE

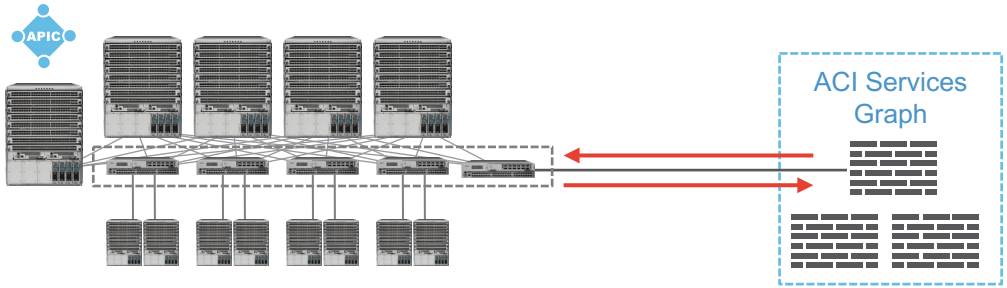



System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, meiroth
ALL TENANTS | Add Tenant | Search: enter name, descr | Meir | Bezeq-int | common | IAF | infra
Tenant Meir
Quick Start
Tenant Meir
Application Profiles
ASAvFailover
MyApp1
Application EPGs
EPG App
Domains (VMs and Bare-M...
Static Bindings (Paths)
Static Bindings (Leaves)
Contracts
Static EndPoint
Subnets
L4-L7 Virtual IPs
L4-L7 IP Address Pool
L4-L7 Service Parameters
EPG DB
EPG web
uSeg EPGs
L4-L7 Service Parameters
Networking
L4-L7 Service Parameters
Security Policies
Contracts
RMI
SQL
Display a menu
Application Profile - MyApp1
Topology
Policy
Stats
Health
Faults
History
100
Drag and drop to configure:
Contract
EPG
µEPG
VZ Any
Baremetal
VM Ware
Microsoft
Openstack
L2
L3
Policies
web (FW)
rmi
sql
Internet
web
App
DB
Groups
Flexible association
SUBMIT
CANCEL


System
Tenants
Fabric
VM Networking
L4-L7 Services
Admin
Operations
Advanced Mode
welcome, meiroth
ALL TENANTS | Add Tenant | Search: enter name, descr | Meir | Bezeq-int | common | IAF | infra
Tenant Meir
Application Profile - MyApp1
Quick Start
Tenant Meir
Application Profiles
ASAvFailover
MyApp1
Application EPGs
EPG App
Domains (VMs and Ba
Static Bindings (Paths)
Static Bindings (Leave
Contracts
Static EndPoint
Subnets
L4-L7 Virtual IPs
L4-L7 IP Address Pool
L4-L7 Service Parame
EPG DB
EPG web
uSeg EPGs
L4-L7 Service Parameters
Networking
L4-L7 Service Parameters
Security Policies
Contracts
RMI
SQL
Display a menu
STEP 2 > Graph
1. Contract
2. Graph
3. ASAv-Routed Parameters
Stats
Health
Faults
History
Config A Service Graph
Device Clusters
Meir /ASAv-Routed (Managed Firewall)
Graph Template:
Meir/SG1
Consumer
EPG
Internet
C
ASAv-Routed
N1
P
Provider
EPG
web
ASAv-Routed Information
Firewall: routed
Profile: FunctionProfile1
Consumer Connector
Type: General
Route Peering
BD: Meir/BD-out
The Bridge Domain that connects the two devices
Cluster Interface: External
Provider Connector
Type: General
Route Peering
BD: Meir/BD1
The Bridge Domain that connects the two devices
Cluster Interface: Internal
menu
PREVIOUS
NEXT
CANCEL
Groups
Flexible association
V
V
V
B
SUBMIT
CANCEL

ACI Security

Automated Security With Built In Multi-Tenancy



Distributed Stateless Firewall

Line Rate Security Enforcement

Open: Integrate Any Security Device

PCI, FIPS, CC, UC-APL, USG-v6

Symantec · SOURCEfire · Check Point SOFTWARE TECHNOLOGIES LTD. · radware Smart Network. Smart Business. · paloalto NETWORKS · intel Security · FORTINET

Embedded Security

- White-list Firewall Policy Model
- RBAC rules
- Hardened CentOS 7.2
- Authenticated Northbound API (X.509)
- Encrypted Intra-VLAN (TLS 1.2)
- Secure Key-store for Image Verification

Micro-Segmentation

- Hypervisor Agnostic (ESX, Hyper-V, KVM*)
- Physical, Virtual Machine, Container
- Attribute Based Isolation/Quarantine
- Point and Click Micro-segmentation
- TrustSec-ACI Integration

Security Automation

- Dynamic Service Insertion and Chaining
- Closed Loop Feedback for Remediation
- Centralized Security Provisioning & Visibility
- Security Policy Follows Workloads

Encryption

- Link MACSEC
- INS-SEC Overlay Encryption
- MKA, SAP
- GCM-AES-256/128-XPN
- GCM-AES-256/128

Why Cisco ACI and OpenStack?

Distributed, Scalable Virtual Networking

- Fully distributed Layer 2, anycast gateway, DHCP, and metadata
- Distributed NAT and floating IP address
- Choice of group policy or Neutron API

Hardware-Accelerated Performance

- Automatic VXLAN tunnels at top of rack (ToR)
- No wasted CPU cycles for tunneling

Operations and Telemetry

- Troubleshooting across physical and virtual environments
- Health scores, atomic counters, and capacity planning per tenant network

Integrated Overlay and Underlay

- Fully managed underlay network through Cisco® APIC
- Capability to connect physical servers and multiple hypervisors to overlay networks

Service Chaining

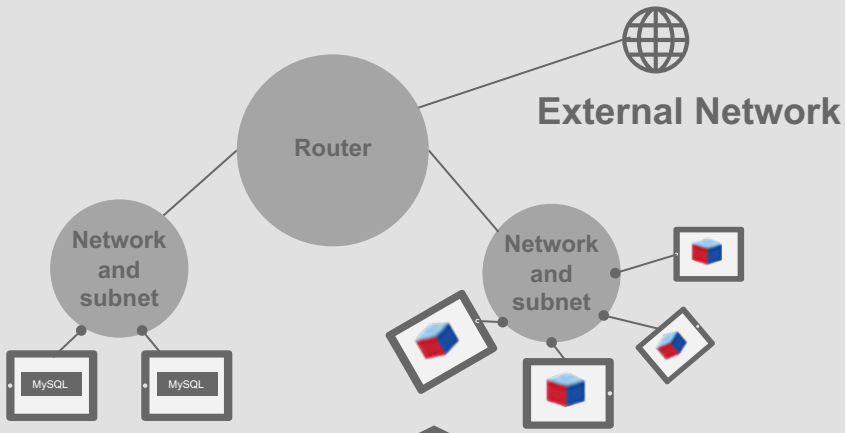
- Support for Layer 3 or Layer 2 service insertion and chaining
- Device package ecosystem for third-party devices or group-based policy (GBP) service chaining

Secure Multitenancy

- Virtual network isolation maintained even when a hypervisor is compromised

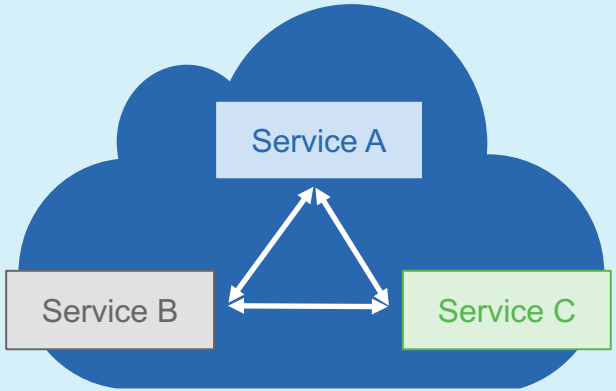
What's Wrong with OpenStack Networking Today?

Neutron Model



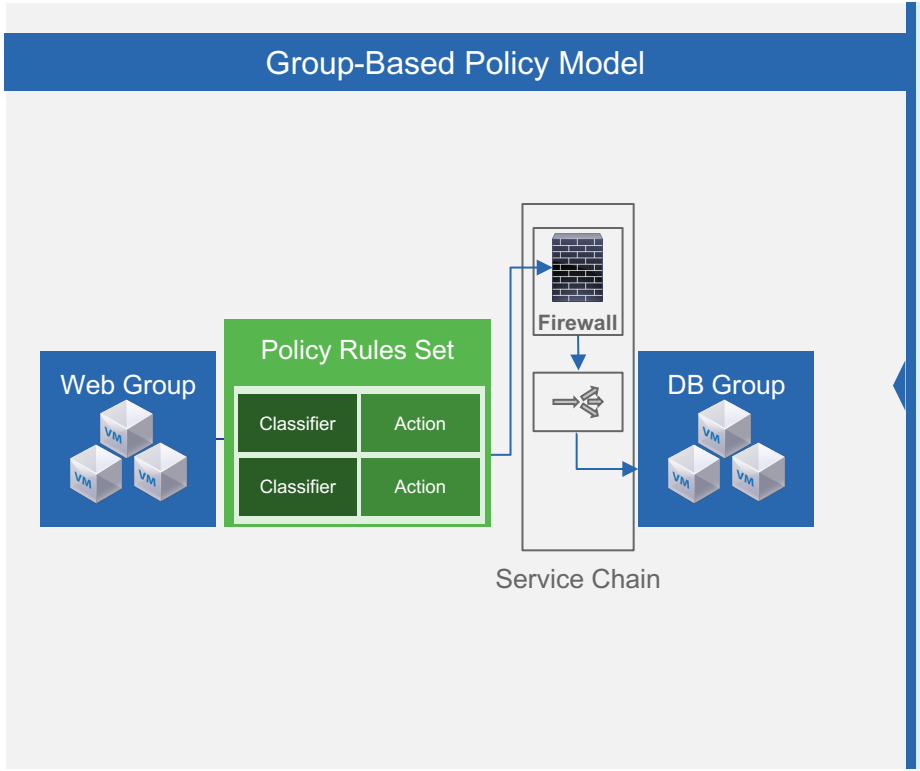
- Layer 2 and broadcast is the base API
- Network, routers, and subnets
- Based on existing networking models
- No concept of dependency mapping or intent

Cloud Application Model



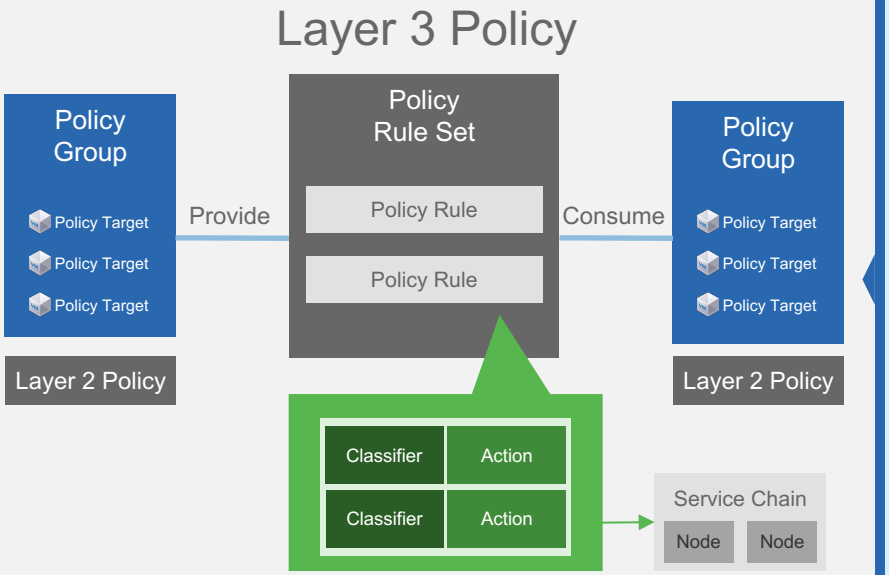
- No broadcast or multicast
- Resilient and fault tolerant
- Scalable tiers
- Built around loosely coupled services
- Does not care about IP addresses

Group-Based Policy for OpenStack



- 100% open source and Apache licensed
- Interface for capturing application intent, including network service requirements
- Model inspired by Cisco® APIC but available for any hardware or software platform
- Networking today, with plans to cover computing and storage
- Growing number of contributors and ecosystem partners

Group-Based Policy Model



Policy group: Set of endpoints with the same properties; often a tier of an application

Policy rule set: Set of classifiers and actions describing how policy groups communicate

Policy classifier: Traffic filter including protocol, port, and direction

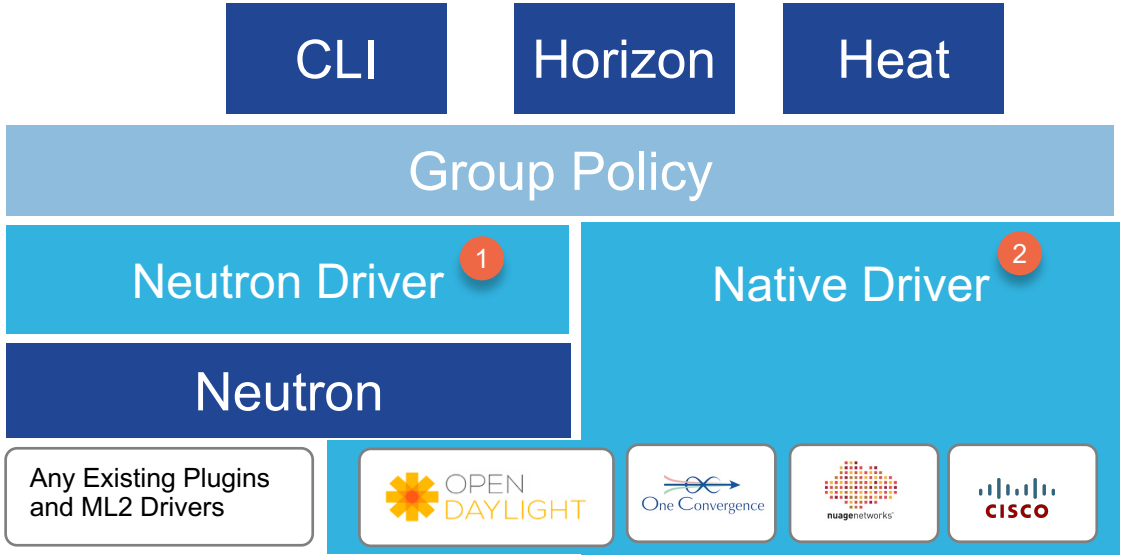
Policy action: Behavior to take as a result of a match; supported actions include **allow** and **redirect**

Service chains: Set of ordered network services between groups

Layer 2 policy: Specification of the boundaries of a switching domain; **broadcast** is an optional parameter

Layer 3 policy: An isolated address space containing Layer 2 policies and subnets

OpenStack GBP Overview

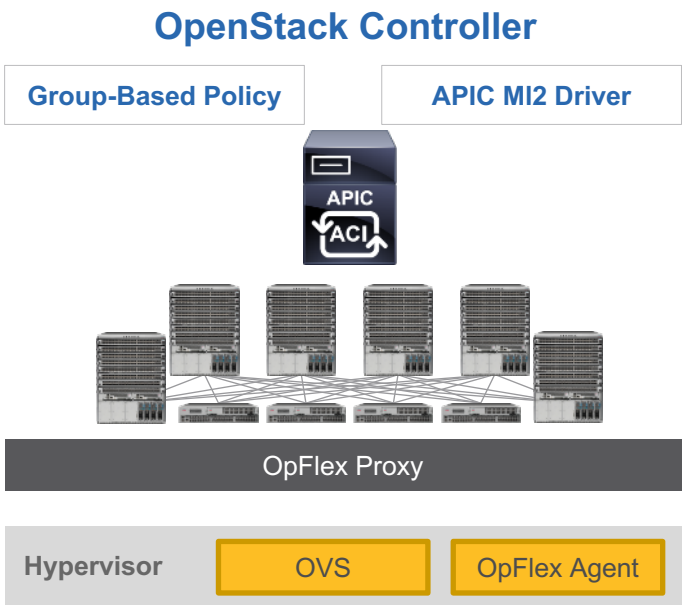


Open model that is compatible with ANY physical or virtual networking backends

1. Neutron Driver maps GBP to existing Neutron API and offers compatibility with any existing Neutron Plugin

2. Native Drivers exist for OpenDaylight as well as multiple vendors (Cisco, Nuage Networks, and One Convergence)

OpFlex Extends Cisco ACI to the Hypervisor



OpFlex for OVS

- Open Source OpFlex agent extends Cisco ACI™ to Linux hypervisor
- OpFlex proxy exposes new open API in Cisco ACI fabric

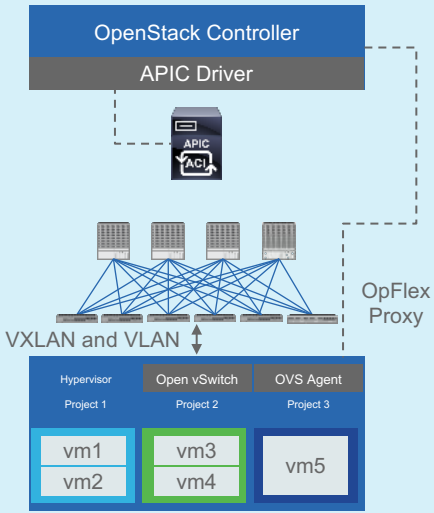
OpenStack Feature Highlights

- Fully distributed Neutron network functions, including Network Address Translation (NAT)
- Integrated, centrally managed overlay and underlay fabric
- Operational visibility integrating OpenStack, Linux, and Cisco® APIC
- Choice of virtual network or group-based policy networking

OpFlex Extends Cisco ACI to the Hypervisor

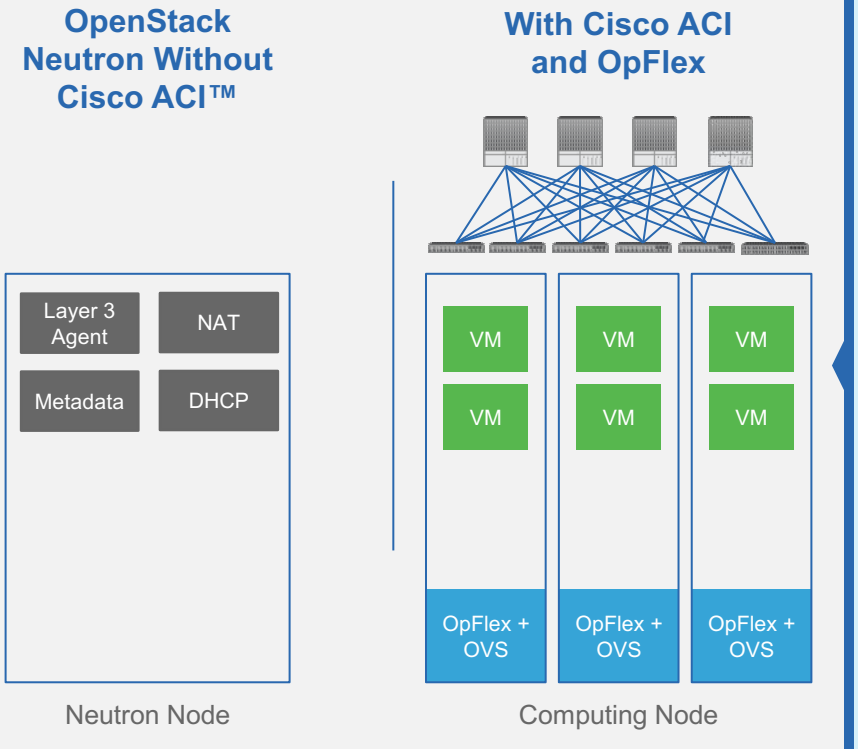
OpFlex and OVS

- VLAN or VXLAN per network and policy group to ToR
- OpFlex proxy runs in leaf, and OpFlex agent manages OVS
- Hypervisor-local traffic has policy and switching, routing handled locally
- VMM domain and GUI integration with APIC
- Distributed support for NAT, metadata server proxies, and DHCP



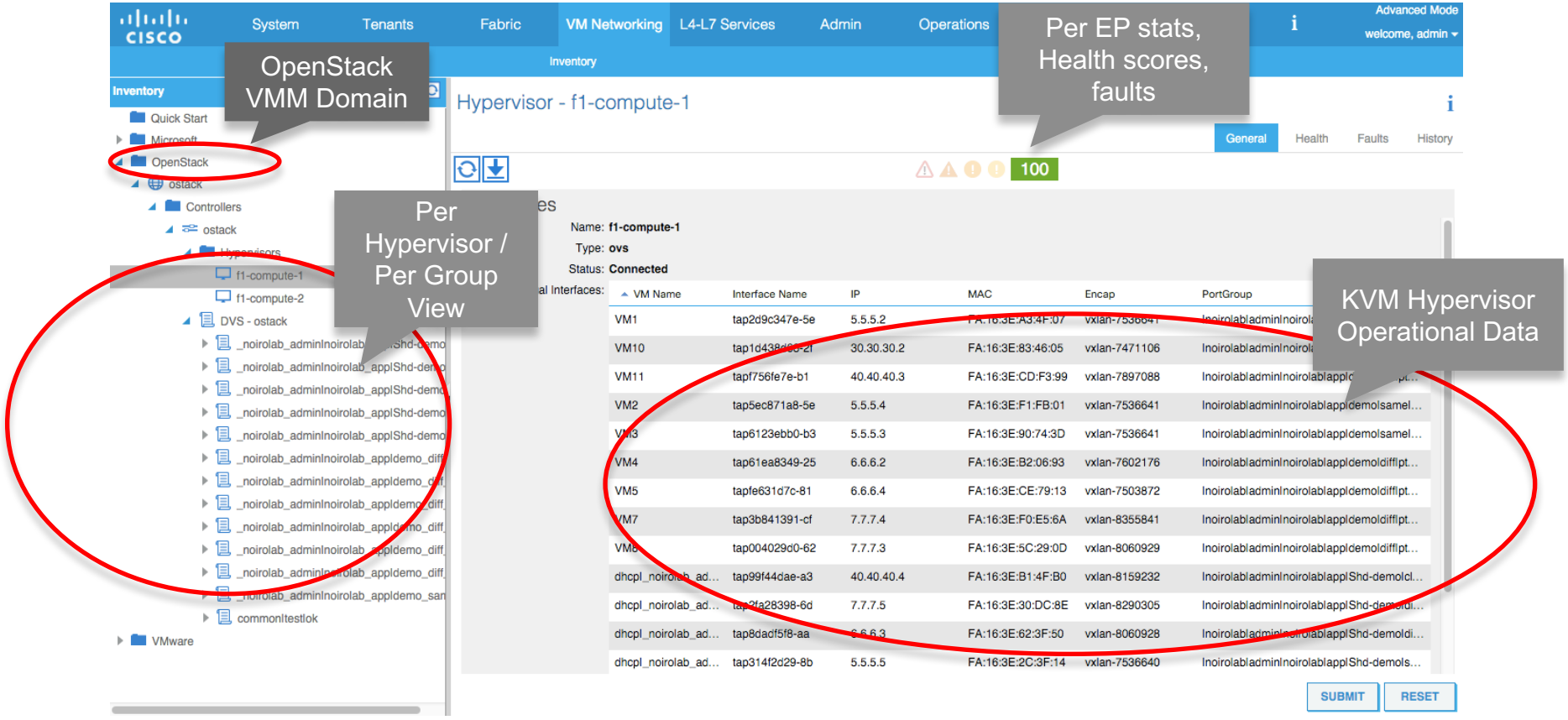
OpFlex agent directly manages OVS and integrates with APIC

Neutron Node High Availability



- Neutron services can be moved from the Neutron node to local computing nodes in a fully distributed manner.
- Critical functions including Layer 3, NAT, metadata proxy, and DHCP can be set up this way (or supported through the network node for traditional support).

APIC VMM Integration



Why Cisco ACI and OpenStack?

Distributed, Scalable Virtual Networking

- Fully distributed Layer 2, anycast gateway, DHCP, and metadata
- Distributed NAT and floating IP address
- Choice of group policy or Neutron API

Hardware-Accelerated Performance

- Automatic VXLAN tunnels at top of rack (ToR)
- No wasted CPU cycles for tunneling

Operations and Telemetry

- Troubleshooting across physical and virtual environments
- Health scores, atomic counters, and capacity planning per tenant network

Integrated Overlay and Underlay

- Fully managed underlay network through Cisco® APIC
- Capability to connect physical servers and multiple hypervisors to overlay networks

Service Chaining

- Support for Layer 3 or Layer 2 service insertion and chaining
- Device package ecosystem for third-party devices or group-based policy (GBP) service chaining

Secure Multitenancy

- Virtual network isolation maintained even when a hypervisor is compromised


CISCO