
JUNIPER NETWORKS
Engineering Simplicity
redhat.
Contrail MultiCloud Security and Analytics for Containers
Technical Overview
Marco Chiandusso, SE Cloud Specialist
#RedHatOSD

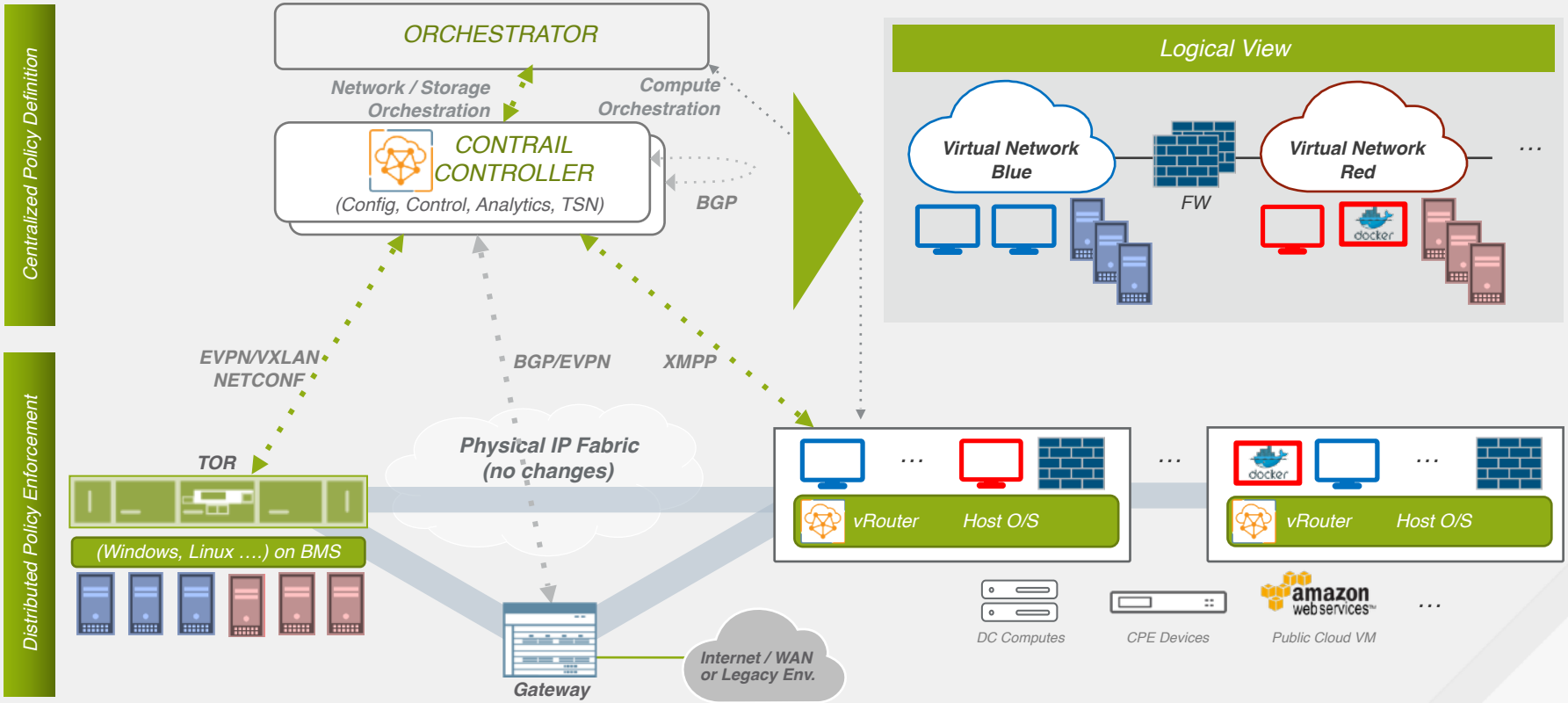
CONFIDENTIALITY AND LEGAL NOTICE

This material contains information that is confidential and proprietary to Juniper Networks, Inc. Recipient may not distribute, copy, or repeat information in the document.

This statement of product direction sets forth Juniper Networks' current intention and is subject to change at any time without notice. No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

Contrail program participants are subject to a license agreement that describes program terms and conditions.

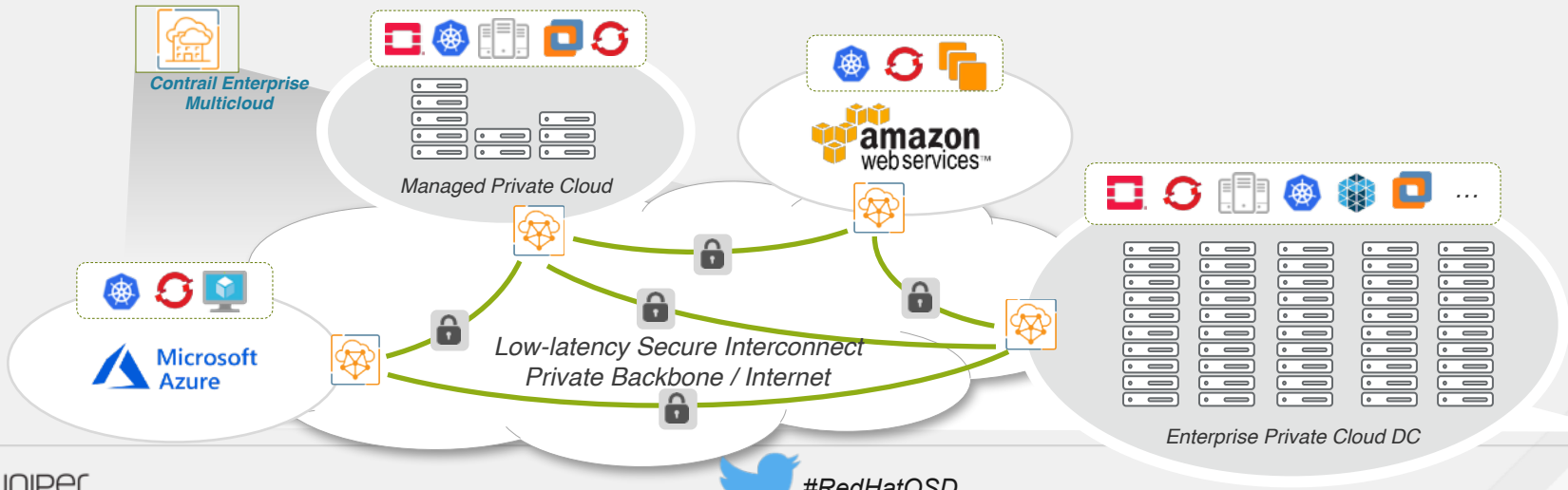
CONTRAIL ARCHITECTURE



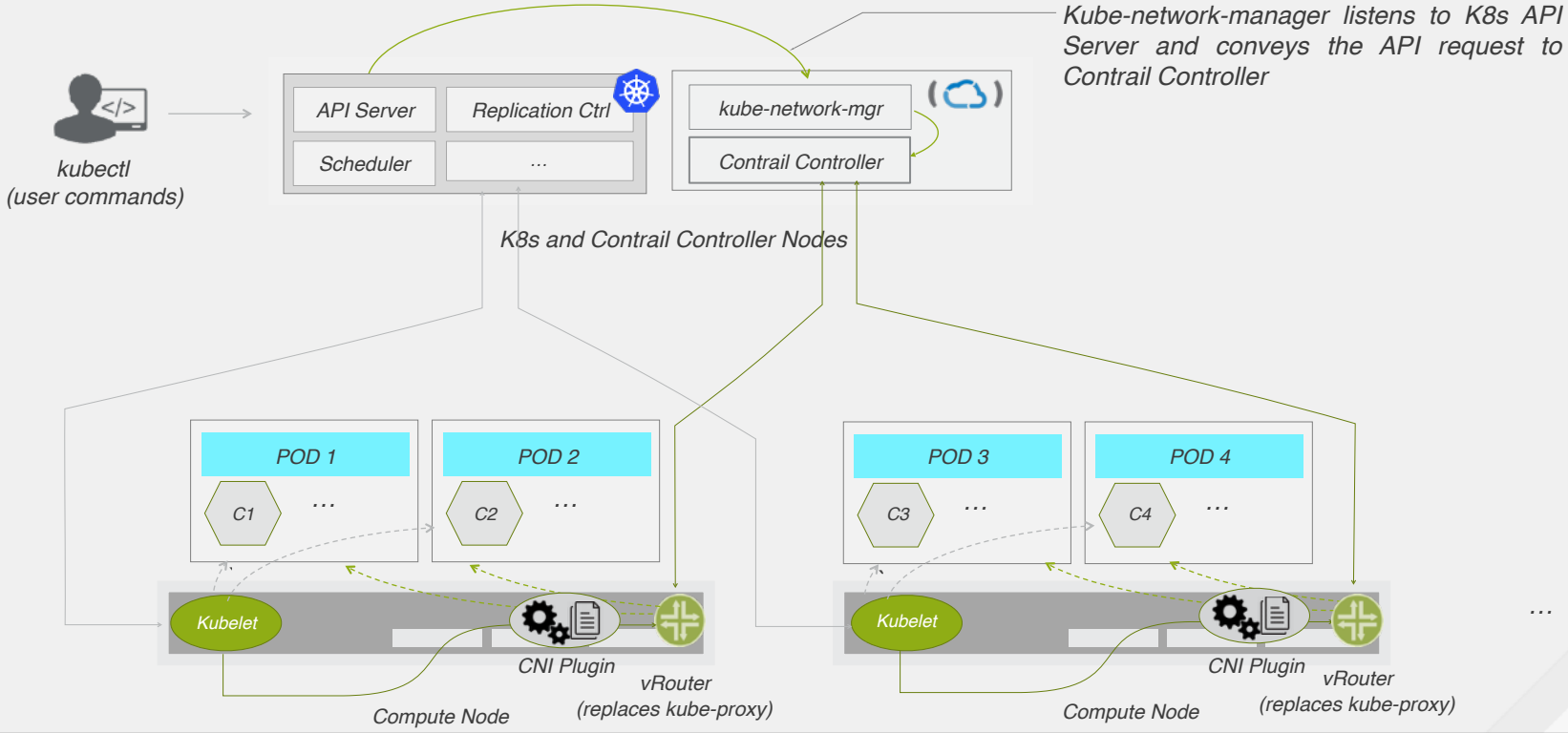
MULTICLOUD INFRA – ENABLING USER-APP INTERACTION

Centralized Network Policy and Security Control

- Connect multiple private and public clouds using an auto-forming mesh of secure tunnels
  - Consume a common network/security interface for all cloud deployments
- Define security policies centrally for all endpoints using dynamic policy generation, and tag based rules
- Manage & Operate cloud networking and security from a single interface



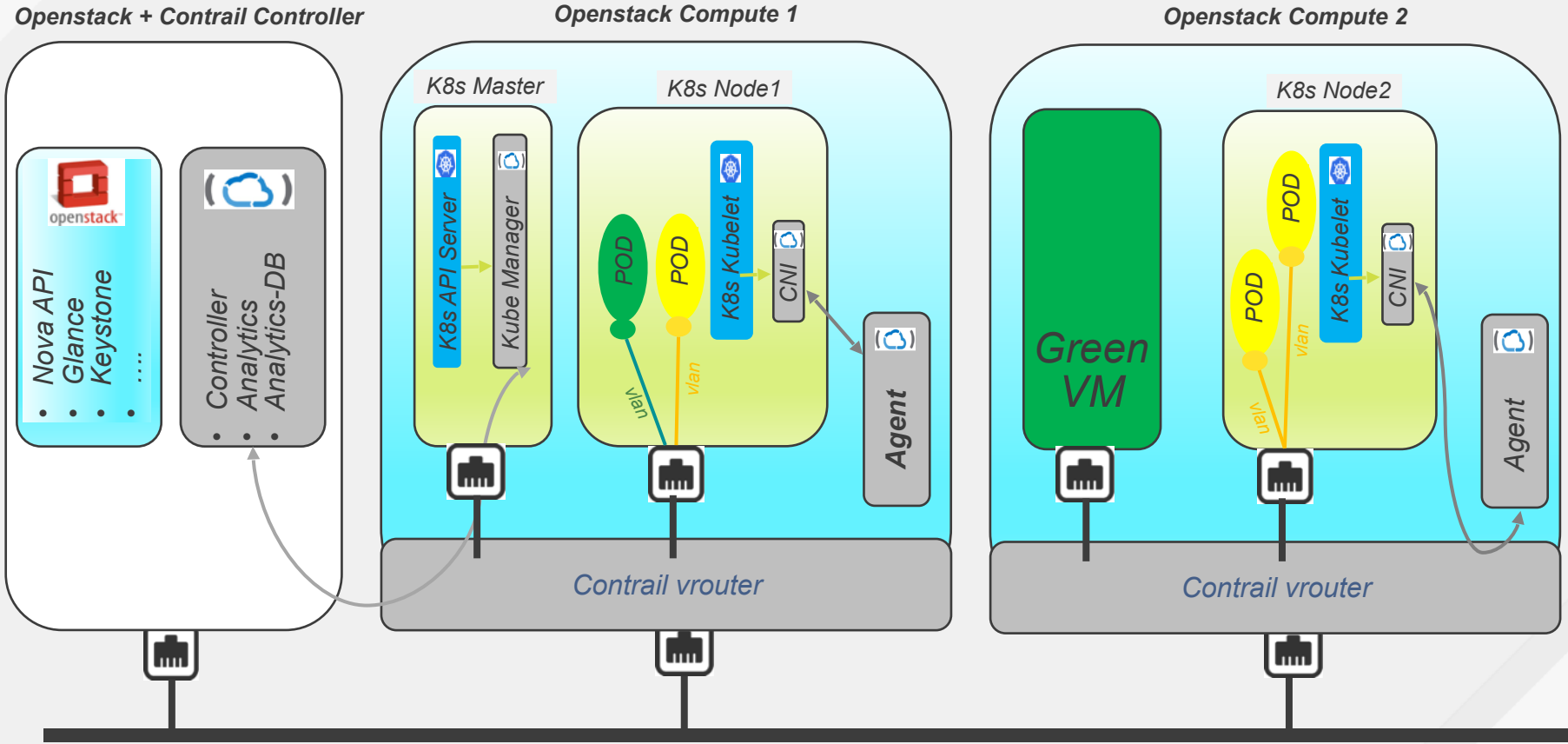
CONTAINERS ARCHITECTURE INTEGRATION



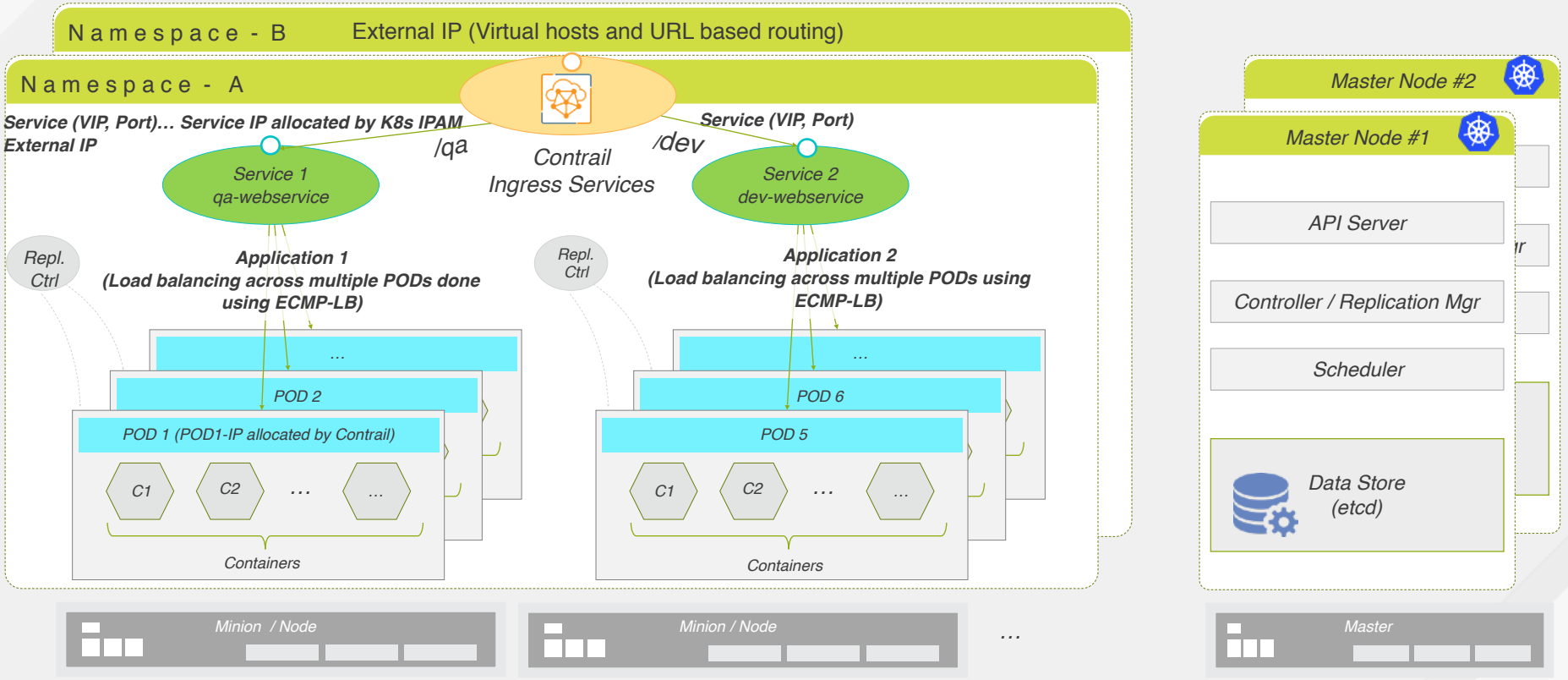
CONTRAIL WITH KUBERNETES ON OPENSTACK
- NESTED MODE

- Contrail provides a collapsed control and data plane in which a single Contrail control plane and a single virtual network stack manage and service both the OpenStack and Kubernetes clusters.
- Single Contrail Controller to provide networking to pods, VMs & baremetal
- Run Kubernetes on OpenStack
  - Launch VMs (K8-master & K8-slave) from OpenStack horizon in a publicly accessible virtual-network
  - Install Kubernetes on the VMs created
  - Create a custom virtual-network. Launch a VM in this network from OpenStack UI & a pod from K8s master node

CONTRAIL WITH KUBERNETES ON OPENSTACK
- DEEP DIVE



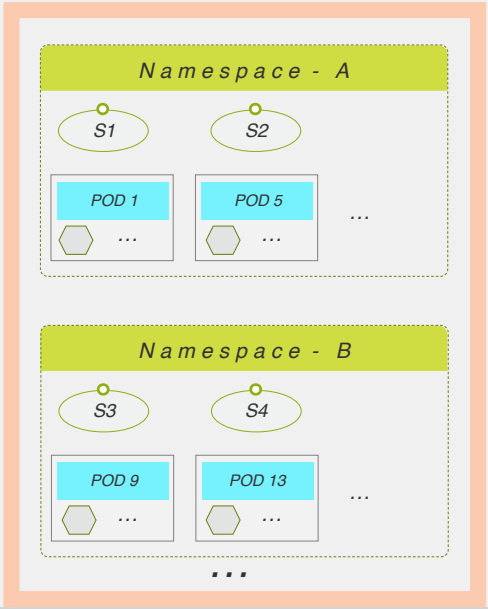
CONTRAIL INGRESS SERVICE AND SERVICE LB



CONTAINER NETWORKING
- DIFFERENT LEVELS OF ISOLATION

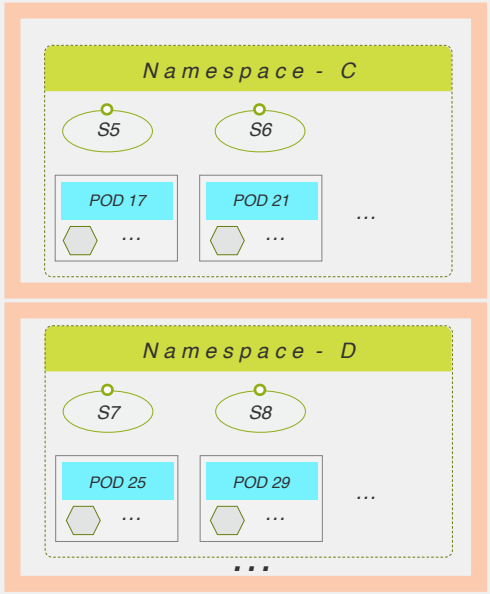
DEFAULT CLUSTER MODE

- This is how K8s networking works today
- Flat subnet where -- Any workload can talk to any other workload



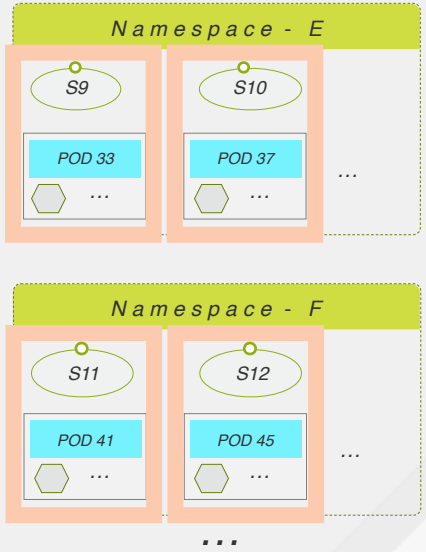
NAMESPACE ISOLATION

- In addition to default cluster, operator can add isolation to different namespaces transparent to the developer



POD / SERVICE ISOLATION

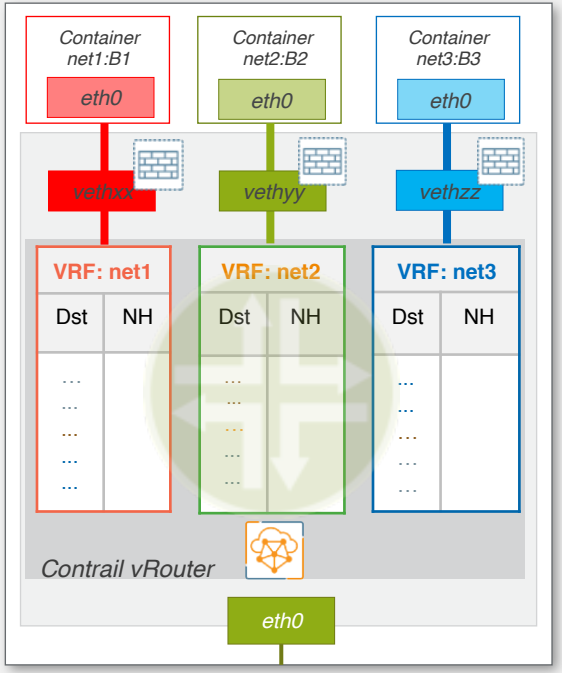
- In this mode, each POD is isolated from one another
- Note that all three modes can co-exist



CONTRAIL AND KUBERNETES NETWORK POLICY

Contrail Security

Per-Interface Microsegmentation



Kubernetes Network Policy is a framework for defining firewall rules via the Kubernetes Manifests

Network Policy defines the rules framework, but not the enforcement. It is up to the CNI to enforce the Network Policy

Rules can be based on Kubernetes labels, to flexibly define firewall filters, or network/port/protocol to define more rigid matches.

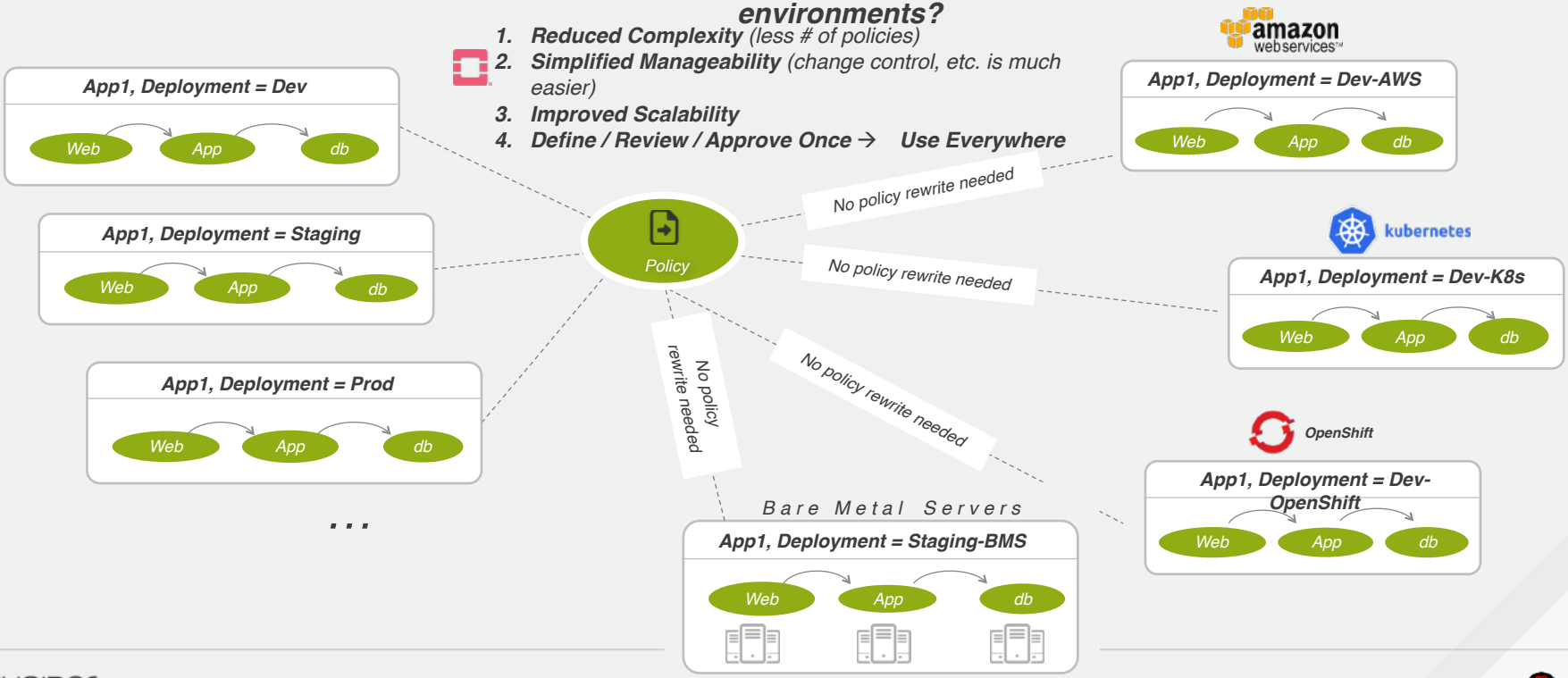
Contrail supports enforcement of Network Policy, extending the label based firewall policy to support OpenStack, VMWare, and Bare Metal

Contrail maintains flow logs, and policy analytics to provide insight and audit support for connected virtual networks.

INTENT-DRIVEN POLICY OPTIMIZATION
- WRITE ONCE – DEPLOY MANY

Once a set of policies are defined for a particular OpenStack environment, they can easily be re-used for other environments?

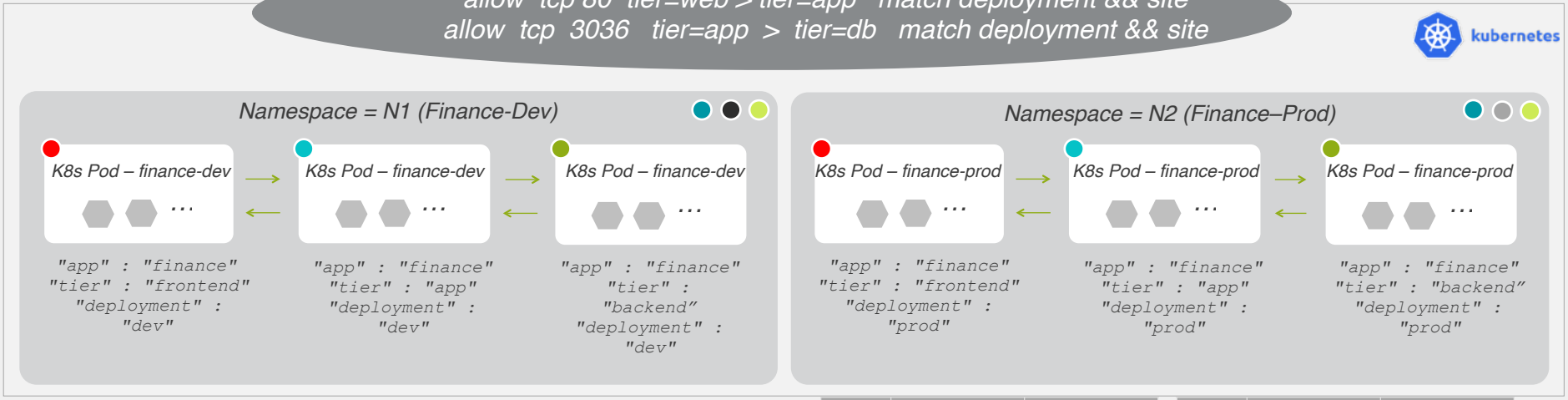
1. ***Reduced Complexity*** *(less # of policies)*
2. ***Simplified Manageability*** *(change control, etc. is much easier)*
3. ***Improved Scalability***
4. ***Define / Review / Approve Once → Use Everywhere***



INTENT-DRIVEN SECURITY POLICY WITH CONTRAIL & K8S

allow tcp 80 tier=web > tier=app match deployment && site
allow tcp 3036 tier=app > tier=db match deployment && site

kubernetes



	Tags	Values
	tier	web
	tier	app
	tier	db
	application	finance
	Custom Global labels	

	Tags	Values
	deployment	dev
	deployment	staging
	deployment	prod
	site	US
	site	EMEA

JUNIPER NETWORKS

redhat

MANAGING THE CLOUD

Applications & Services

Cloud Infrastructure

Software Defined Infrastructure

Physical Infrastructure

Software Defined Operations

Stream analysis to monitor SLAs and predict faults

Cross Layer Visibility

Real-time optimizations to improve efficiency and ensure service availability

CONTRAIL VALUE PROP FOR CONTAINERIZED ENVIRONMENTS

Create secure multi-tenant container environments, with existing application developer workflow

Offer multiple deployment options (i.e. bare metal server, Private / Public Clouds, etc.)

Seamless migration & interop of existing Contrail (non-container) environments with a container environment

Extend all vRouter features (QoS, Floating IP, DDI, etc.) to a container environment

Allow Operator to modify infra security (& isolation) levels, transparent to app developer


JUNIPER NETWORKS
Engineering Simplicity
redhat.
GRAZIE PER L'ATTENZIONE
MARCO CHIANDUSSO – SE CLOUD SPECIALIST
#RedHatOSD