

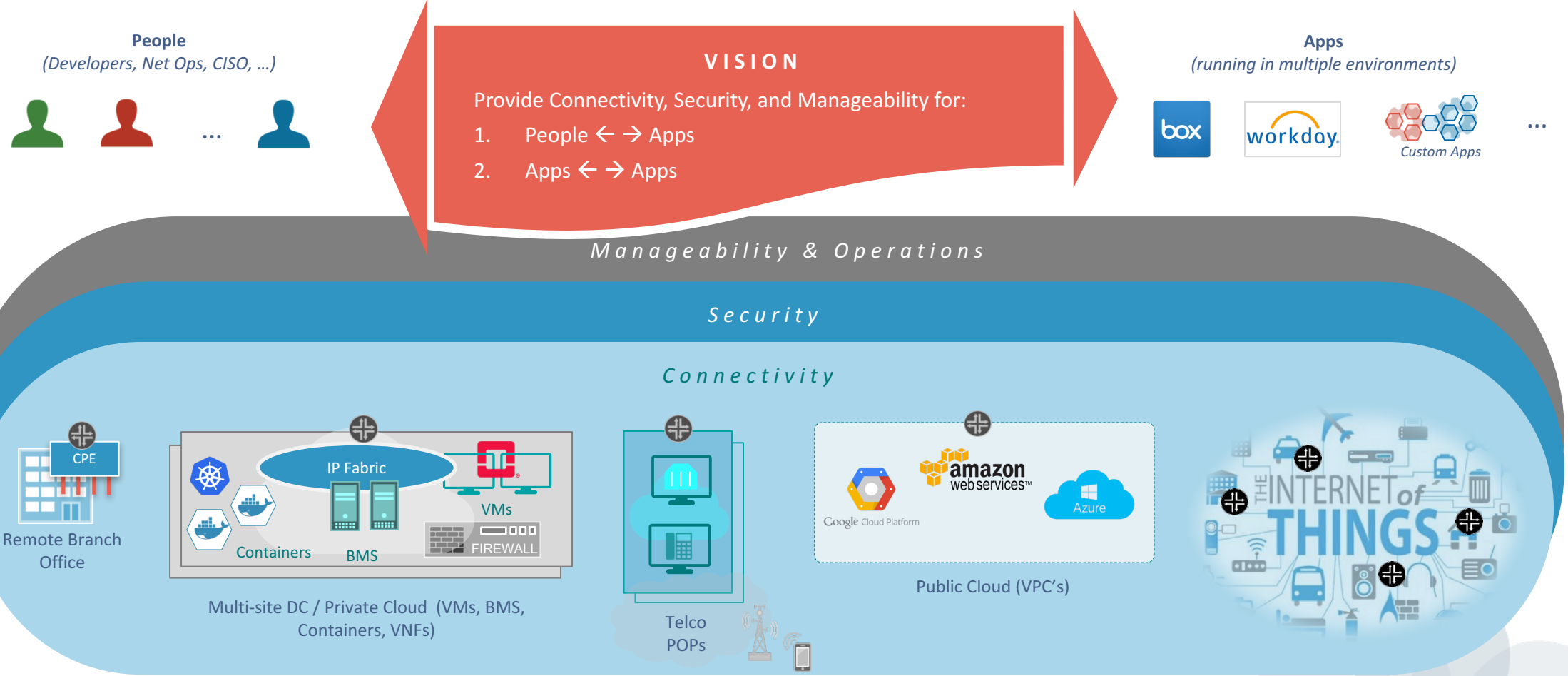
# Security and Analytics for Cloud made easy by Contrail and Appformix

---

November 2017

Marco Chiandusso, Consultant Engineer

# CONTRAIL VISION: GOALS & OBJECTIVES



# Challenges of Traditional Security Paradigm

## Or “The Security Scale Challenge in Multi Cloud Environments”



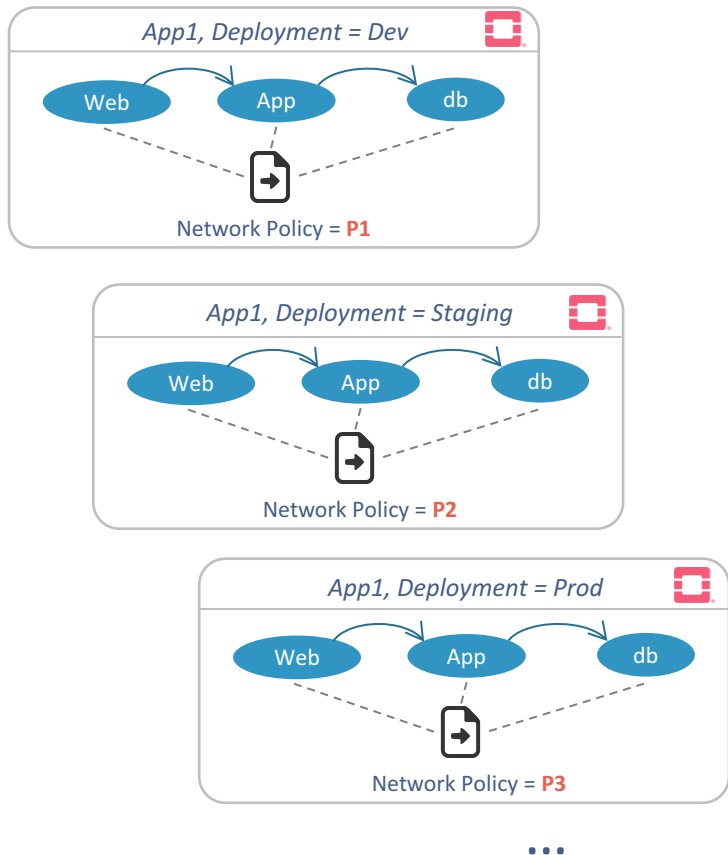
- Security is Perimeter based – but perimeter is everywhere
- Explosion in # of apps, endpoints, environments on the one hand
- Explosion in # of threats, malware, spyware, hacking, attacks, data leaks on the other hand
- Results in Policy explosion – management complexity and nightmare
- Manual, error prone and non-automated. Does not scale.



# Consistent Intent- Driven Policies

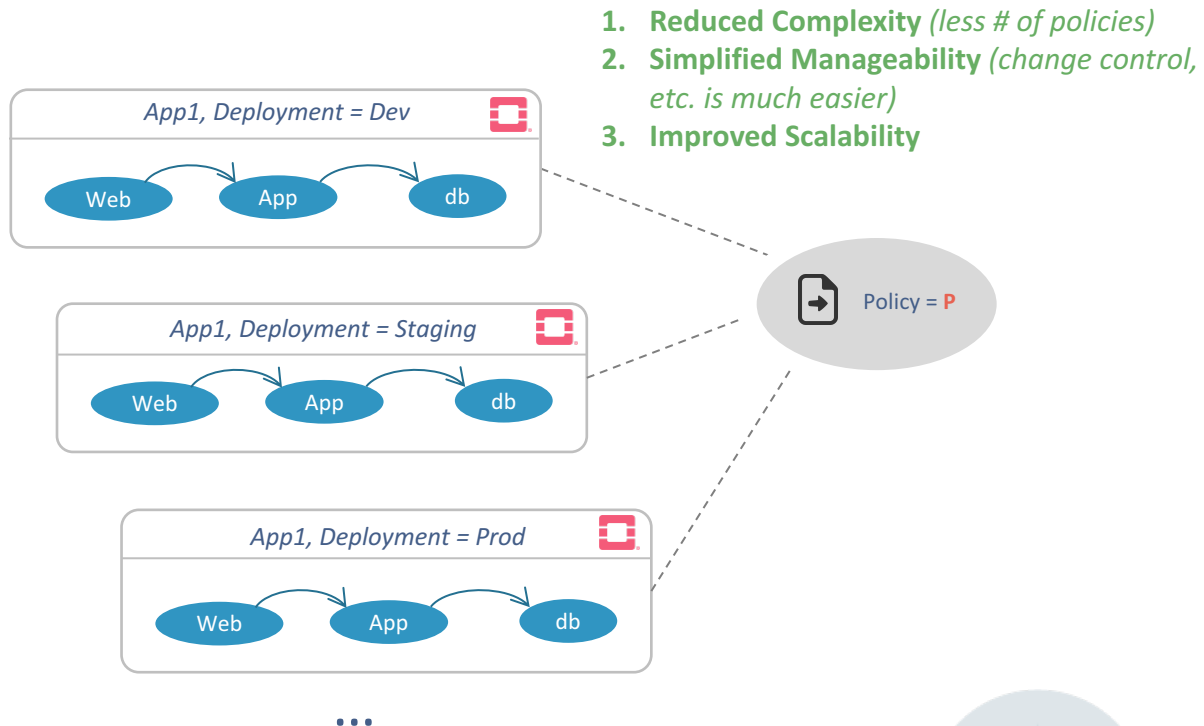
# Single Policy, Multiple Environments

## Current Behavior



## Desired Behavior

Can we use one policy to be applied in all the different deployments ?

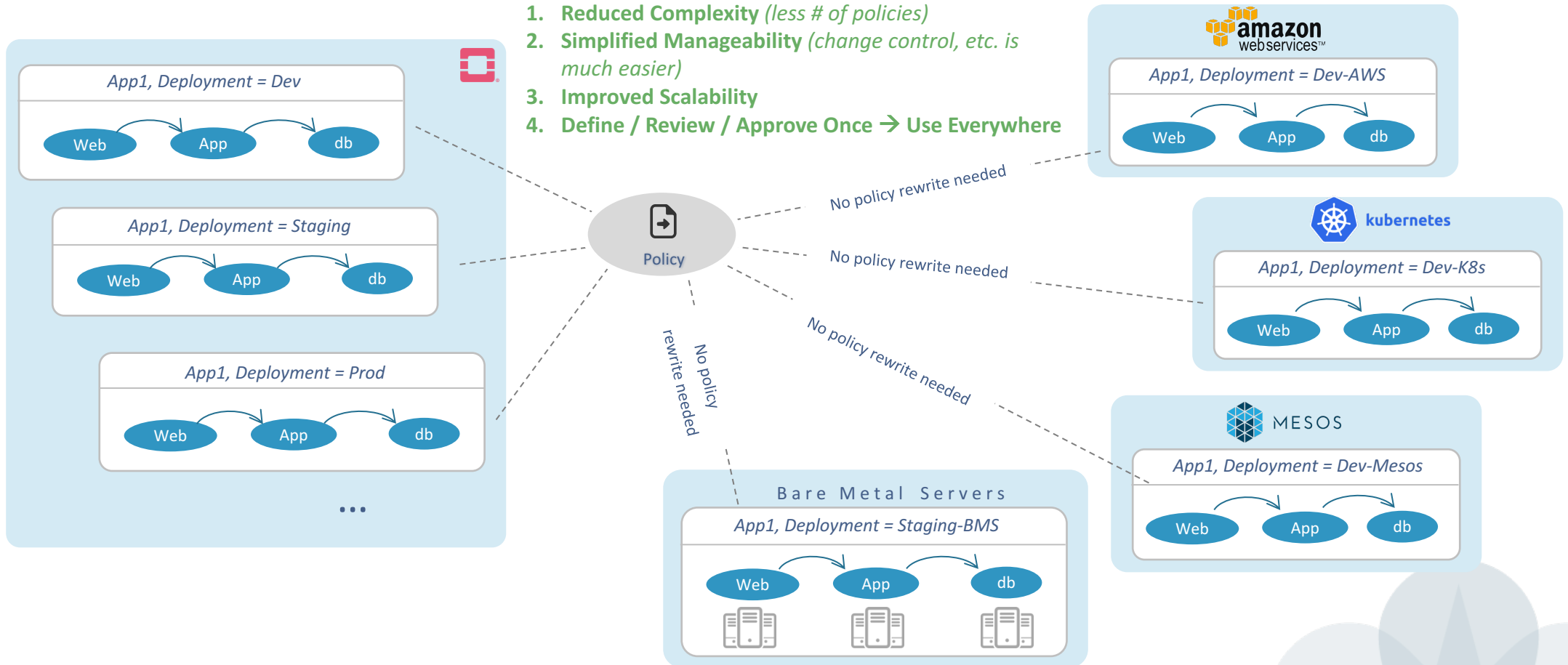


1. **Reduced Complexity** (*less # of policies*)
2. **Simplified Manageability** (*change control, etc. is much easier*)
3. **Improved Scalability**

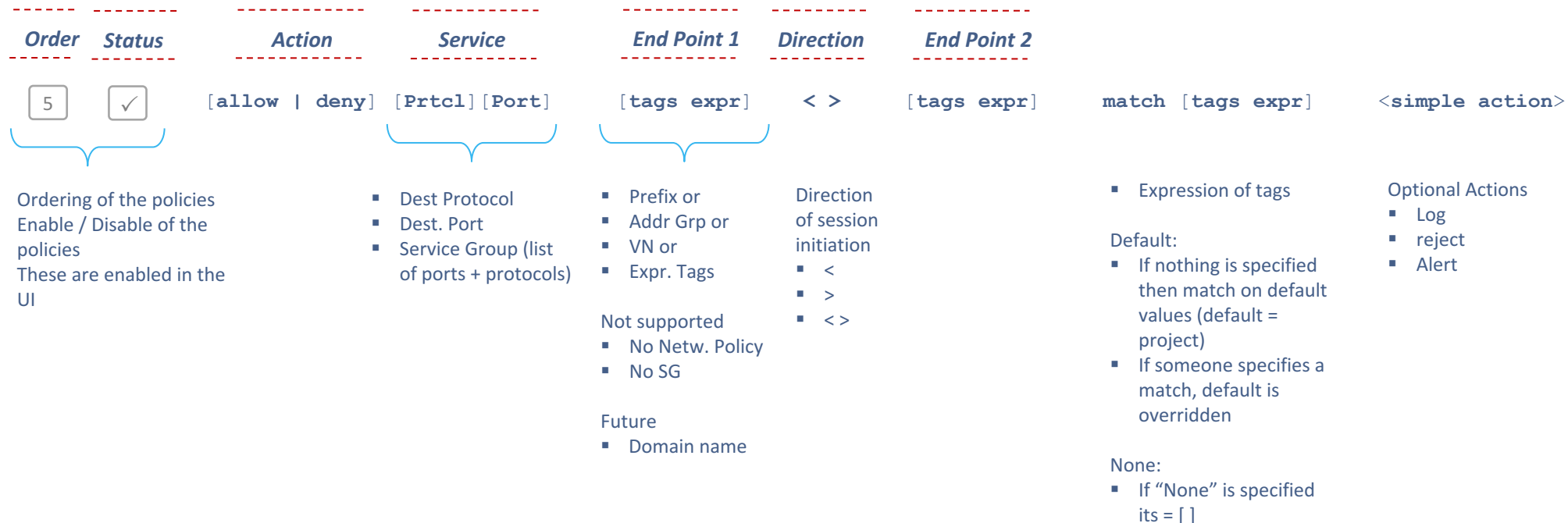
# Consistent Policy - Write Once, Apply Everywhere

Once a set of policies are defined for a particular OpenStack environment, can it be applied to 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 Policy Rule Structure



Tags can be attached to:

Global, Project, Network, VM/BMS/Container, VMI

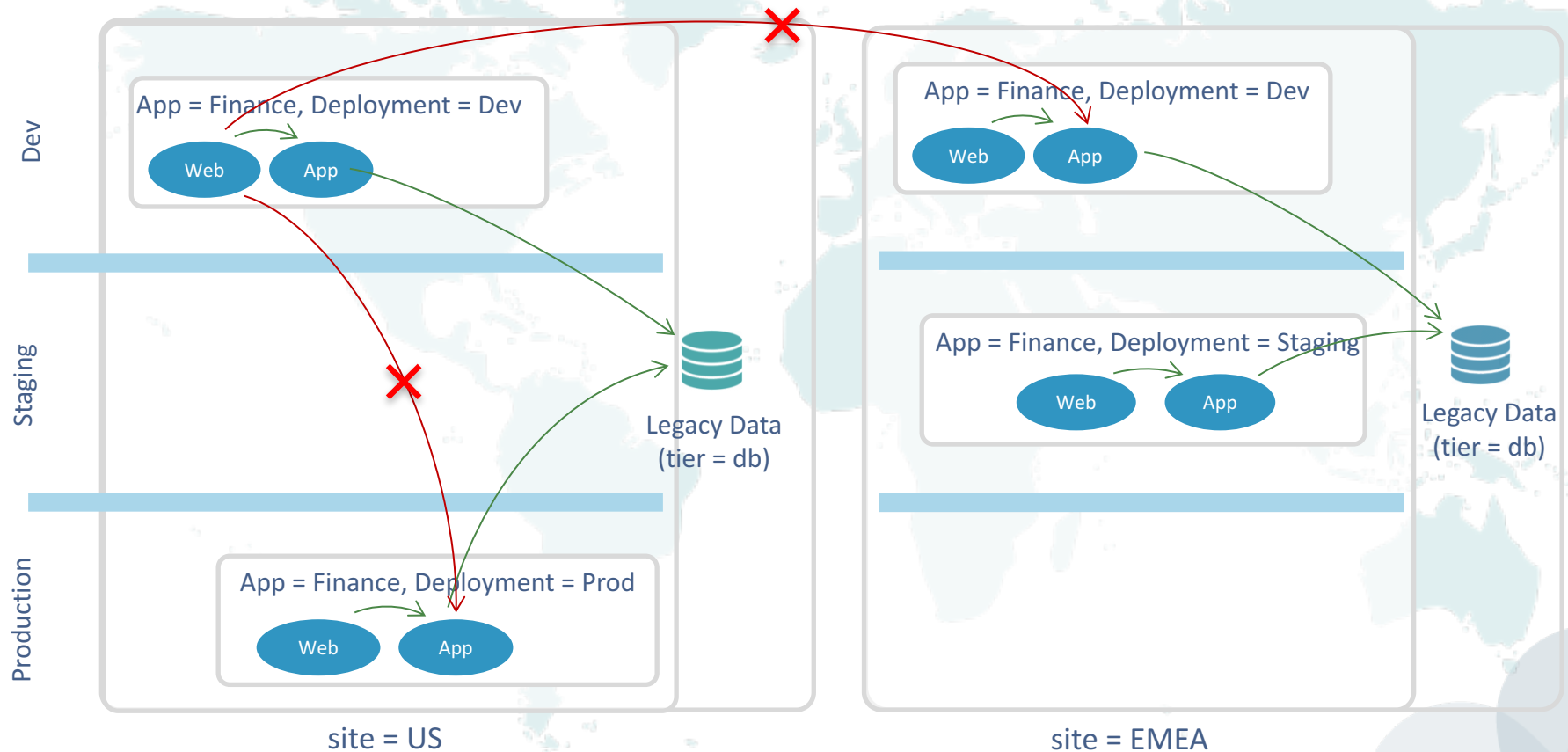
Policies enforced at interface level

# Intent-Driven Policy Framework

Defn

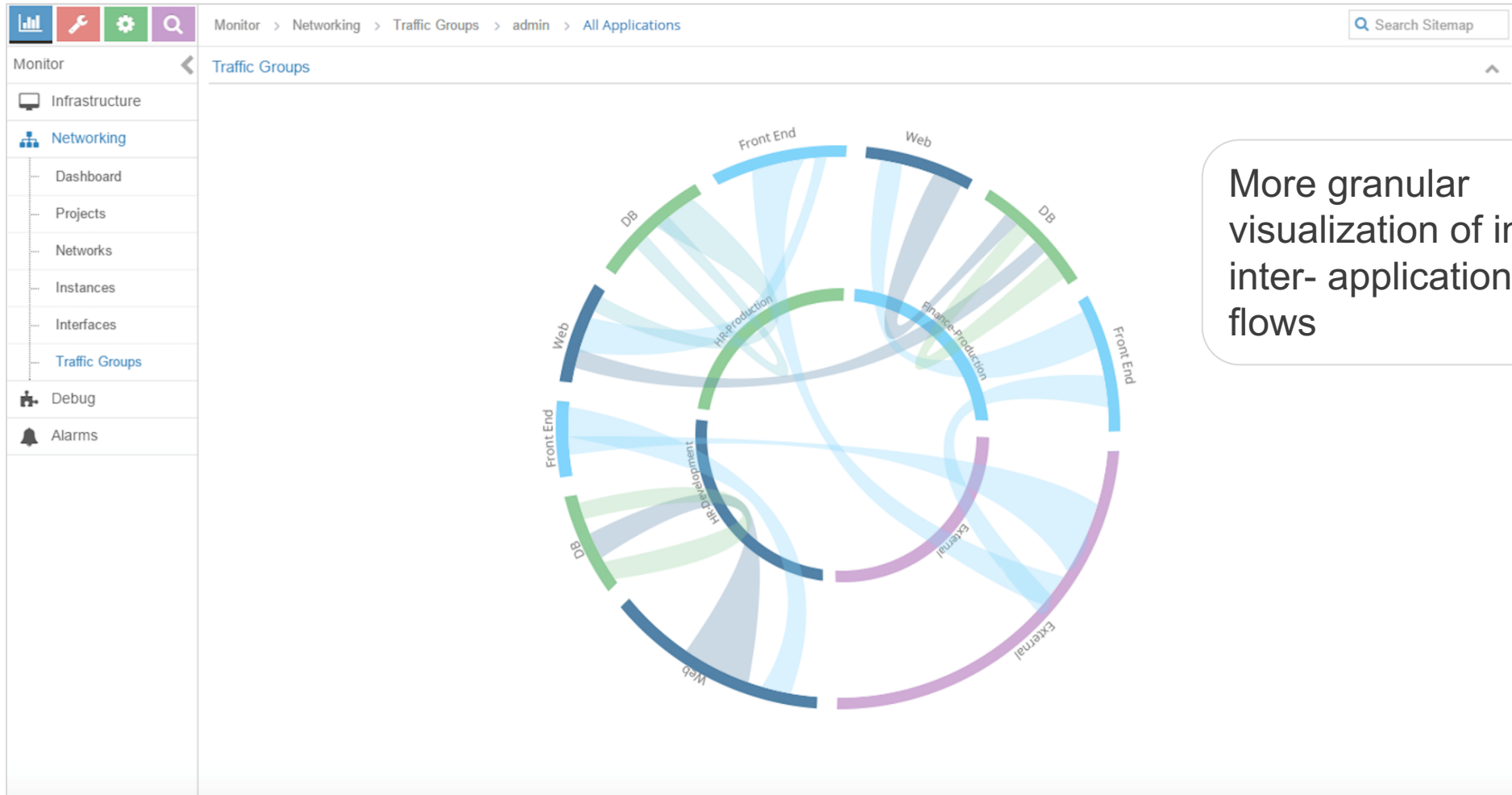
- 1 allow web-service tier=web > tier=app match deployment && site
- 2 allow db-service tier=app > tier=db match site

Enforcement





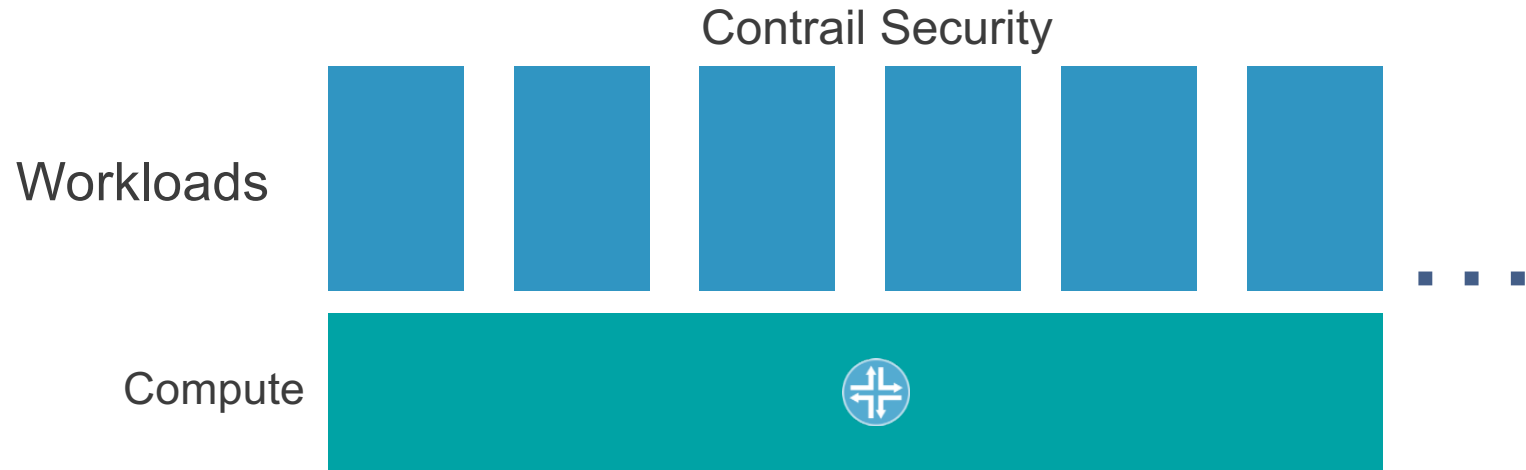
# Contrail Security Applications Flow



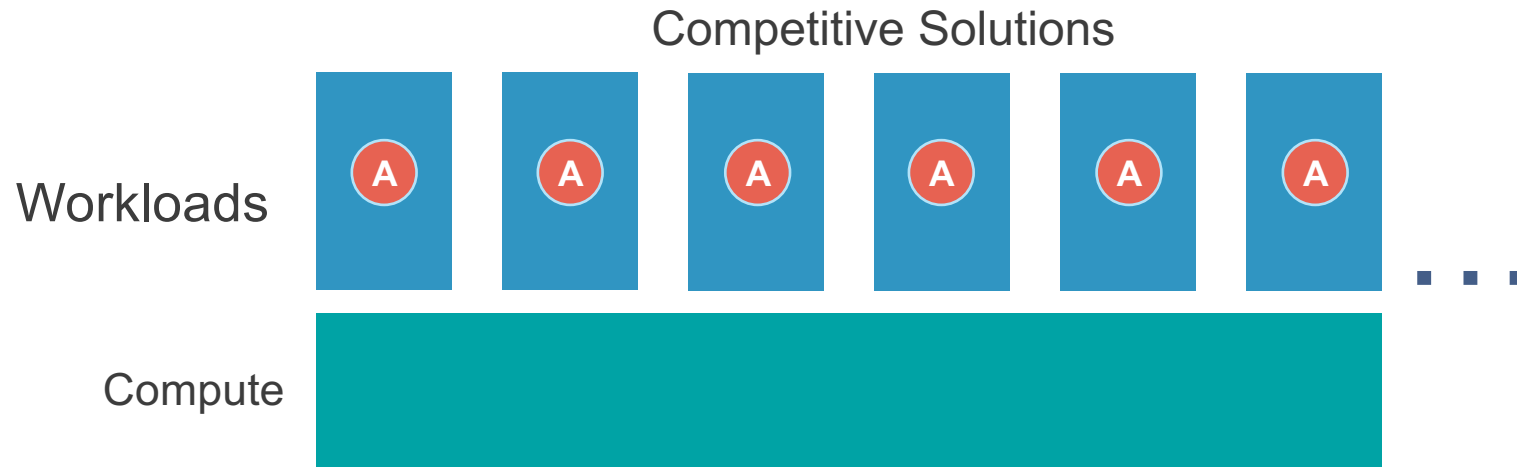
More granular visualization of intra- and inter- application traffic flows

# Multiple Enforcement Points

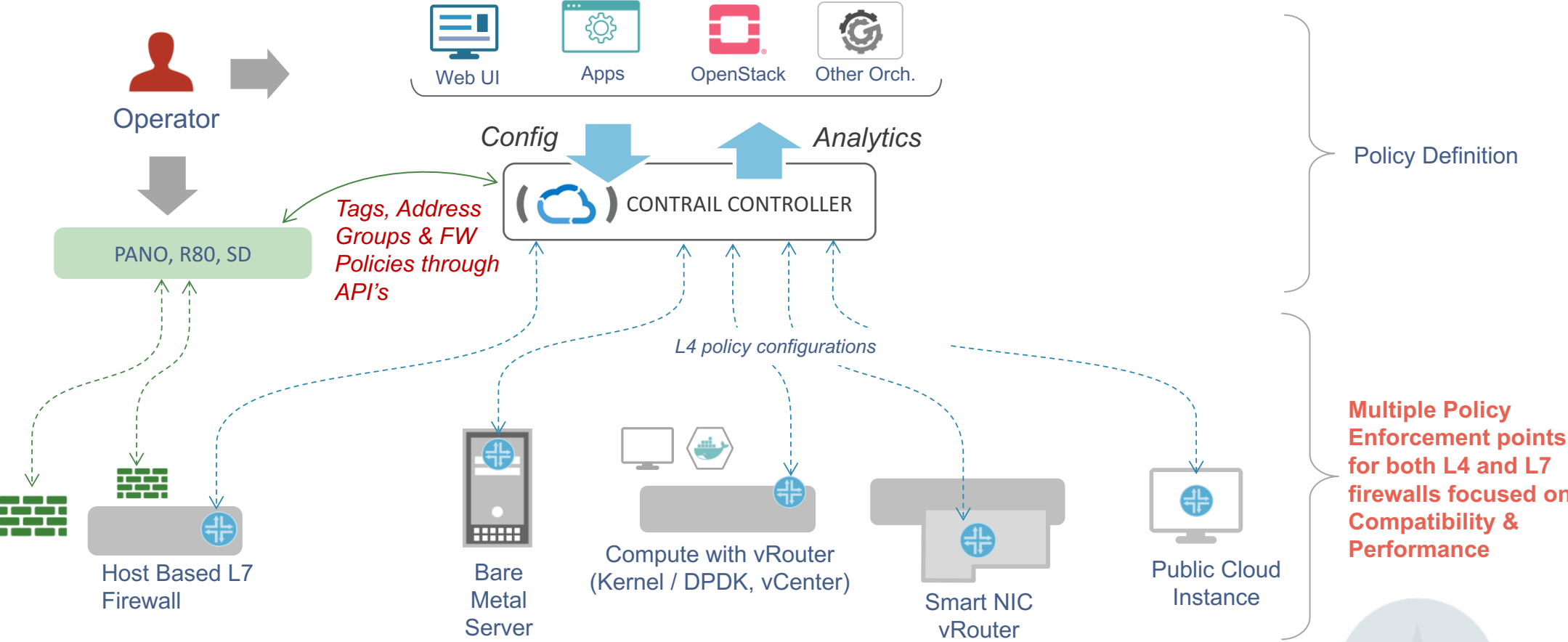
# No Need for Agents in Every Workload



Less # of agents to manage  
=  
more scalable solution



# Multiple Enforcement Points



3<sup>rd</sup> Party or Juniper FW

vRouter enforcing L4 policies and sending traffic to L7 FW for advanced security services

# Conrail Security Summary

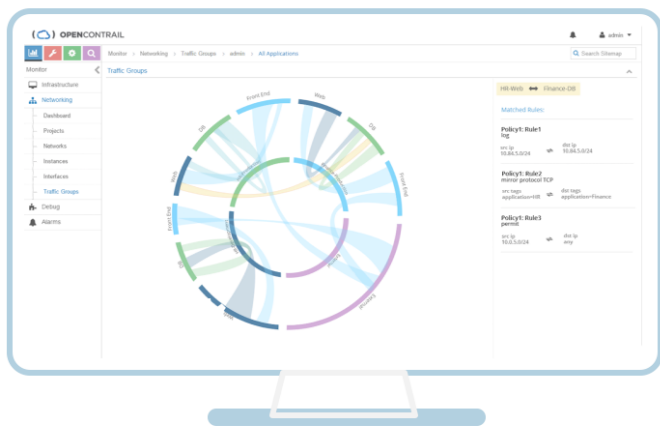
# The Solution - Contrail Security

## Application Security Across Hybrid & Multi-Clouds



### Application Flow Visualization

Discover Inter- and Intra-application traffic flows without enforcing policies



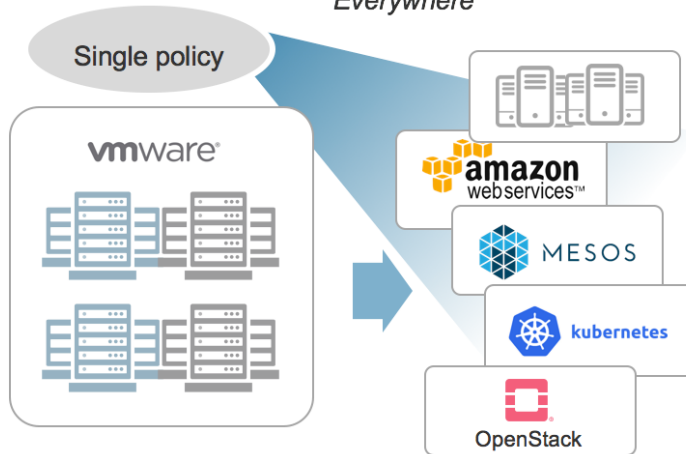
- Offer visualization, analytics, and orchestration for security configurations
- Provide reporting, troubleshooting and compliance



### Consistent Automated Intent-driven Policy



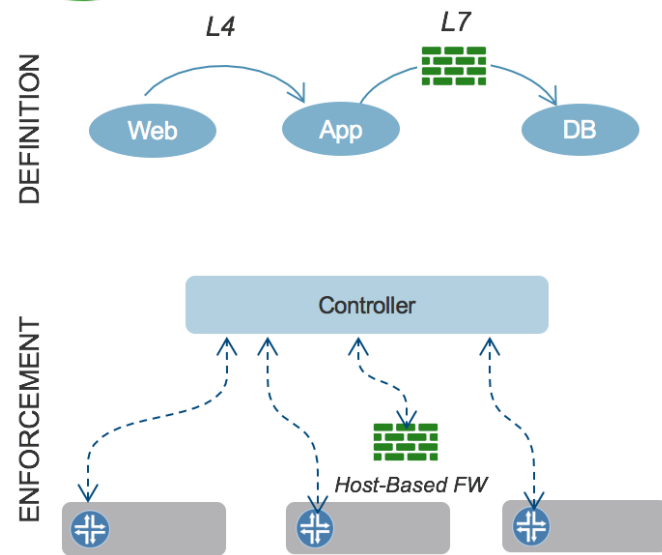
No Policy Rewrite ... Define Once → Enforce Everywhere



- How to extend the same set of policies to Mesos, AWS, Kubernetes, Bare Metal Servers → without policy rule explosion



### Scalable & Performant Multi-point Enforcement



- L4 Enforcement at the vRouter
- L7 enforcement at the L7 Firewall

# Software Defined Operations

## APPFORMIX

**holistic  
ops management**  
(no silos or gaps)

### ANY APPS & SERVICES



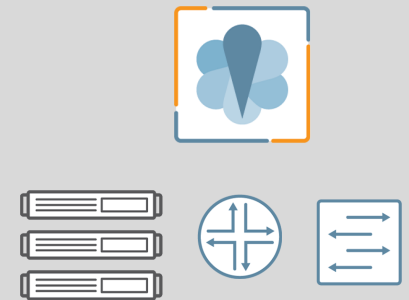
### CLOUD INFRASTRUCTURE



### SOFTWARE-DEFINED INFRASTRUCTURE



### PHYSICAL INFRASTRUCTURE





**Thank you**