

CONTRAIL SECURITY

Aniket Daptari

Sr. Product Manager

Contrail – Cloud Networking & Security

Scott Sneddon

Senior Director

Cloud and SDN

LEGAL DISCLAIMER

This statement of 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.

This presentation contains proprietary roadmap information and should not be discussed or shared without a signed non-disclosure agreement (NDA).

AGENDA

- 1 PROBLEM STATEMENTS (Why)
- 2 PRODUCT OVERVIEW (What)
- 3 POLICY FRAMEWORK (How)

WHY CONTRAIL SECURITY?

Challenges of Traditional Security Paradigm

The Security Scale Challenge



- 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.

What to protect

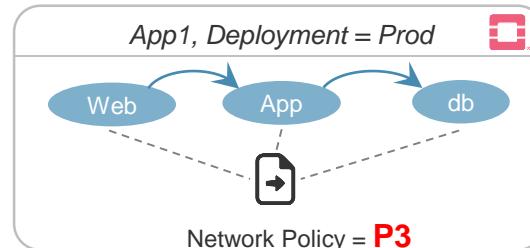
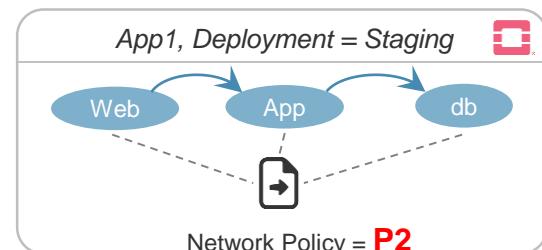
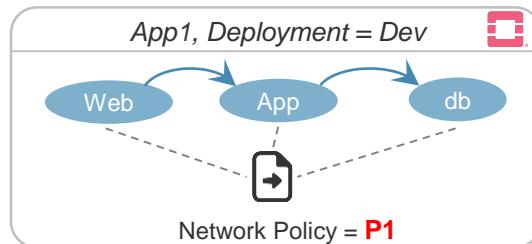
1. Applications
 2. Number of endpoints
 3. Environments – dev, prod, staging, on-prem, public cloud,
 4. ...

What to protect against:

1. Data leaks
 2. DDoS
 3. Malware
 4. Hacks
 5. Viruses
 6. Spyware, etc

PROBLEM STATEMENT

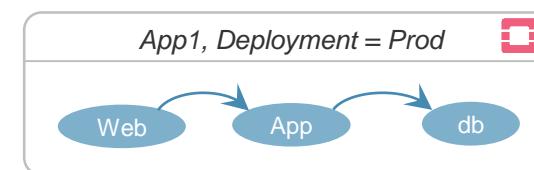
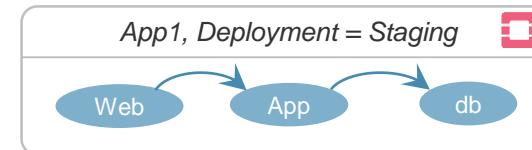
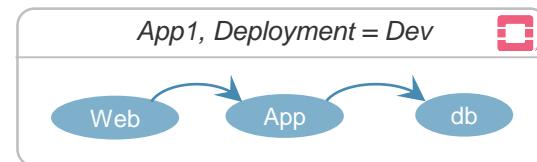
Current Behavior



...

Desired Behavior

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

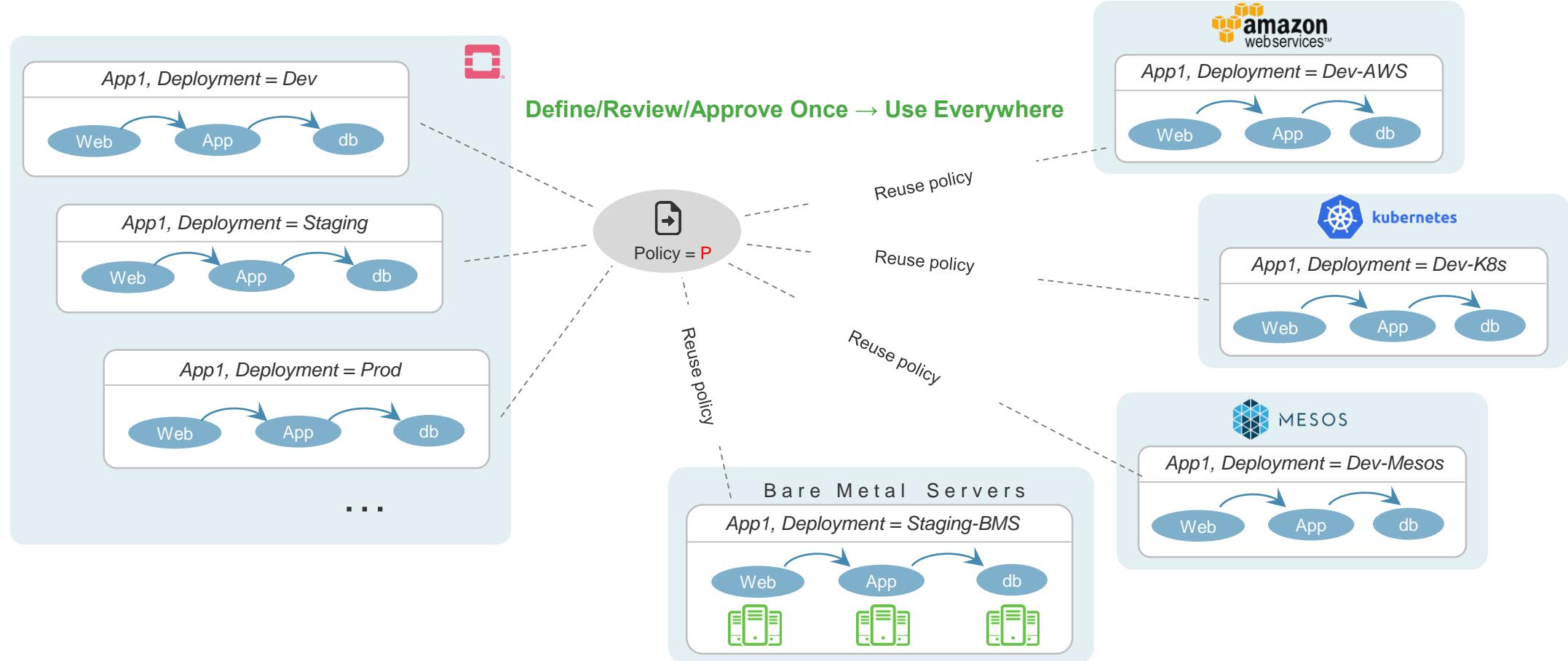


...

- 1. Reduced Complexity
- 2. Simplified Management
- 3. Improved Scalability

PROBLEM STATEMENT

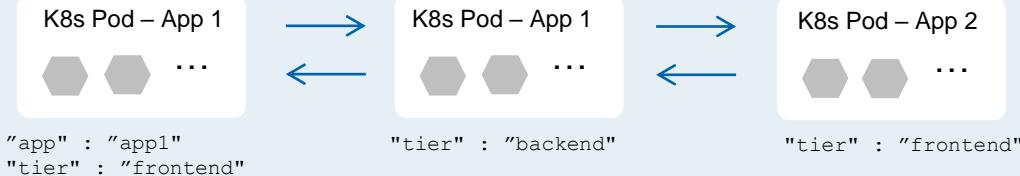
Reuse of policies across multiple clouds and with multiple orchestrators



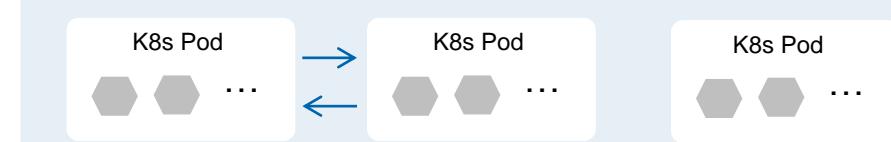
PROBLEM STATEMENT

A Kubernetes application developer creates labels for K8s pods ... Can the security admin overlay his policies transparent to the developer – [i.e. use the same (or different) labels to create security policies / boundaries] ?

Kubernetes Application – created by Developer
(uses different labels to imply connectivity characteristics)

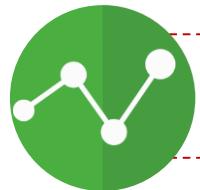


CSO / Compliance / Operators puts policies
(using the same or different labels seamless to developer)



WHAT IS CONTRAIL SECURITY?

CONTRAIL SECURITY KEY CAPABILITIES

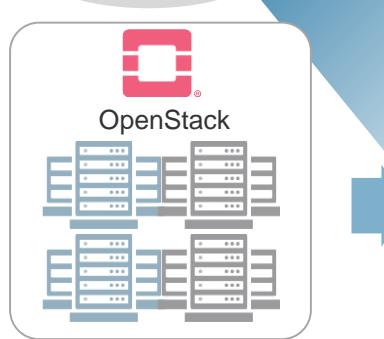


Consistent Intent-Driven Policy



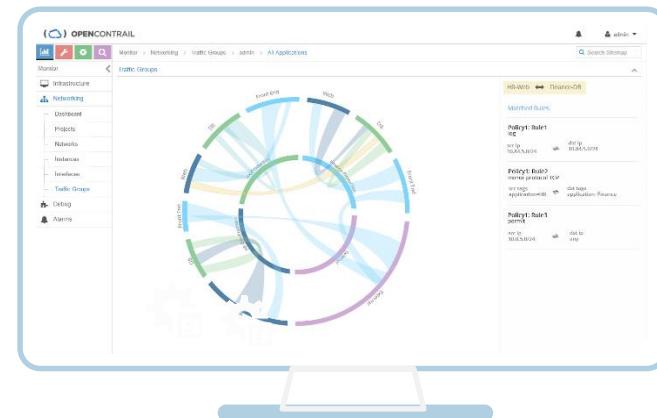
No Policy Rewrite ...
Define Once → Enforce Everywhere

Single policy



Application Policy Config & Flow Visualization

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



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

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



Multiple Enforcement Points

DEFINITION

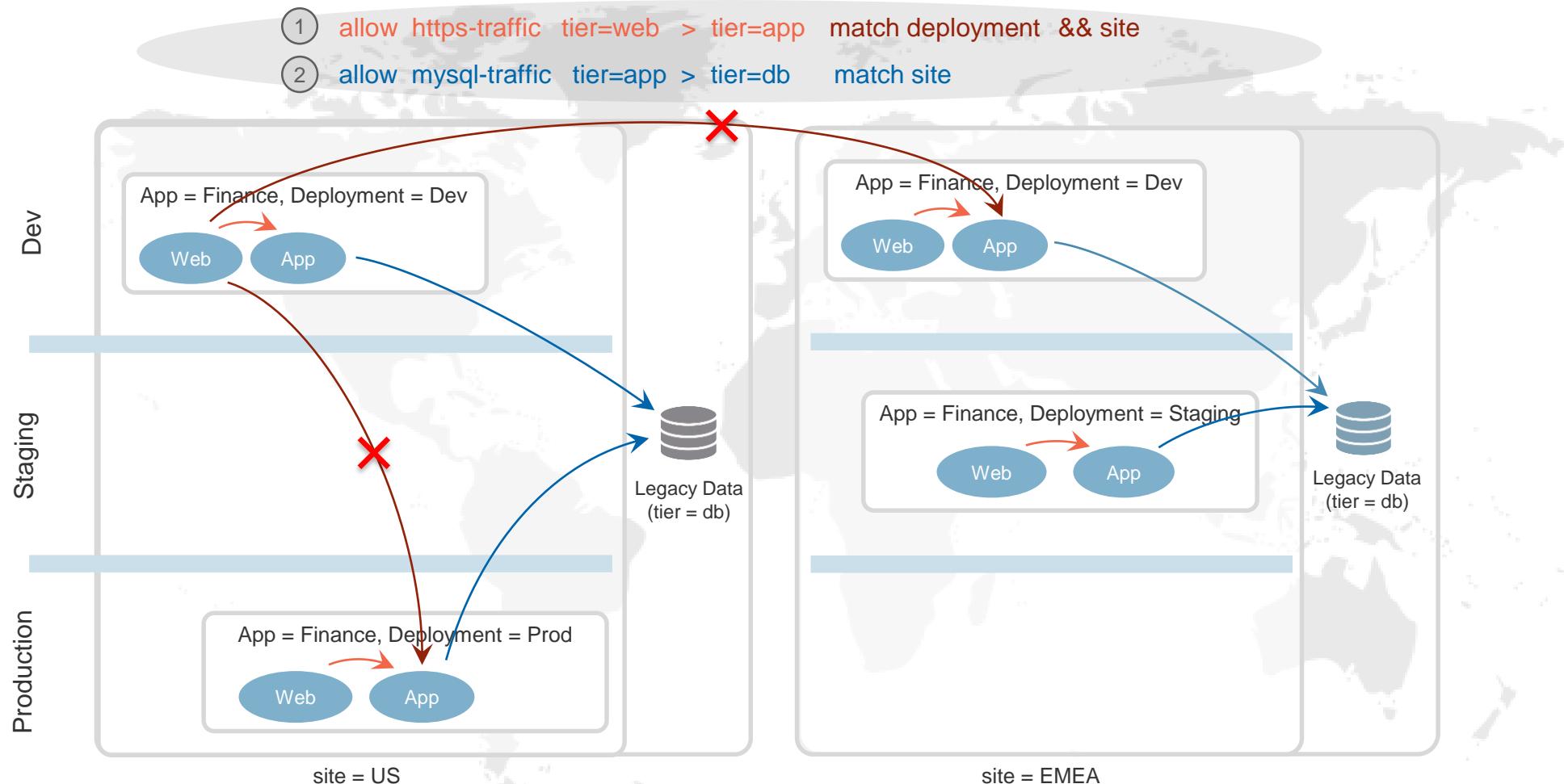


ENFORCEMENT



- L4 Enforcement at the vRouter (Kernel, DPDK, vCenter, Smart NIC)
- L7 enforcement at the L7 Firewall

USE-CASE SCENARIO – POLICY FRAMEWORK



TAGS & OTHER POLICY ITEMS

Various ways to tag the workloads

- 1. Application = HRMS, CRM, ...
- 2. Deployment = Dev, QA, Staging, Production ...
- 3. Site = India, US, EMEA, etc...
- 4. Tier = Web, App, DB,...

- 1. Label = anything custom
- 2. Custom Tags

- User
- User Role
- OS
- Software Compliance
- Customer
-
- Compute Node: e.g. used in affinity / anti-affinity policies for compute
- Rack
- POD
- Cluster
- DC

Phase 1
Deliverables

Roadmap

Address Group

Can be used as an end-point in the policy...

- 1. Prefixes
- 2. Static Group of IP Addresses
- 3. Dynamic Groups with custom labels
- 4. ...

Service Group

List of Protocol & port (e.g. web-service)

- 1. tcp 80
- 2. tcp 8080
- 3. ...

Application Policy Group

*List of policies → make it an application set ...
This helps in easy attachment to any application ...*

- 1. Firewall Policy 1
- 2. Firewall Policy 2
- 3. ...

POLICY – KEY ITEMS TO NOTE

Policy Example: `allow http-traffic tier=web > tier=app match deployment && site`

The diagram shows the policy example with annotations: 'tier=web' and 'tier=app' are labeled 'Tag expression'; 'deployment && site' is labeled 'Tag key expression'.



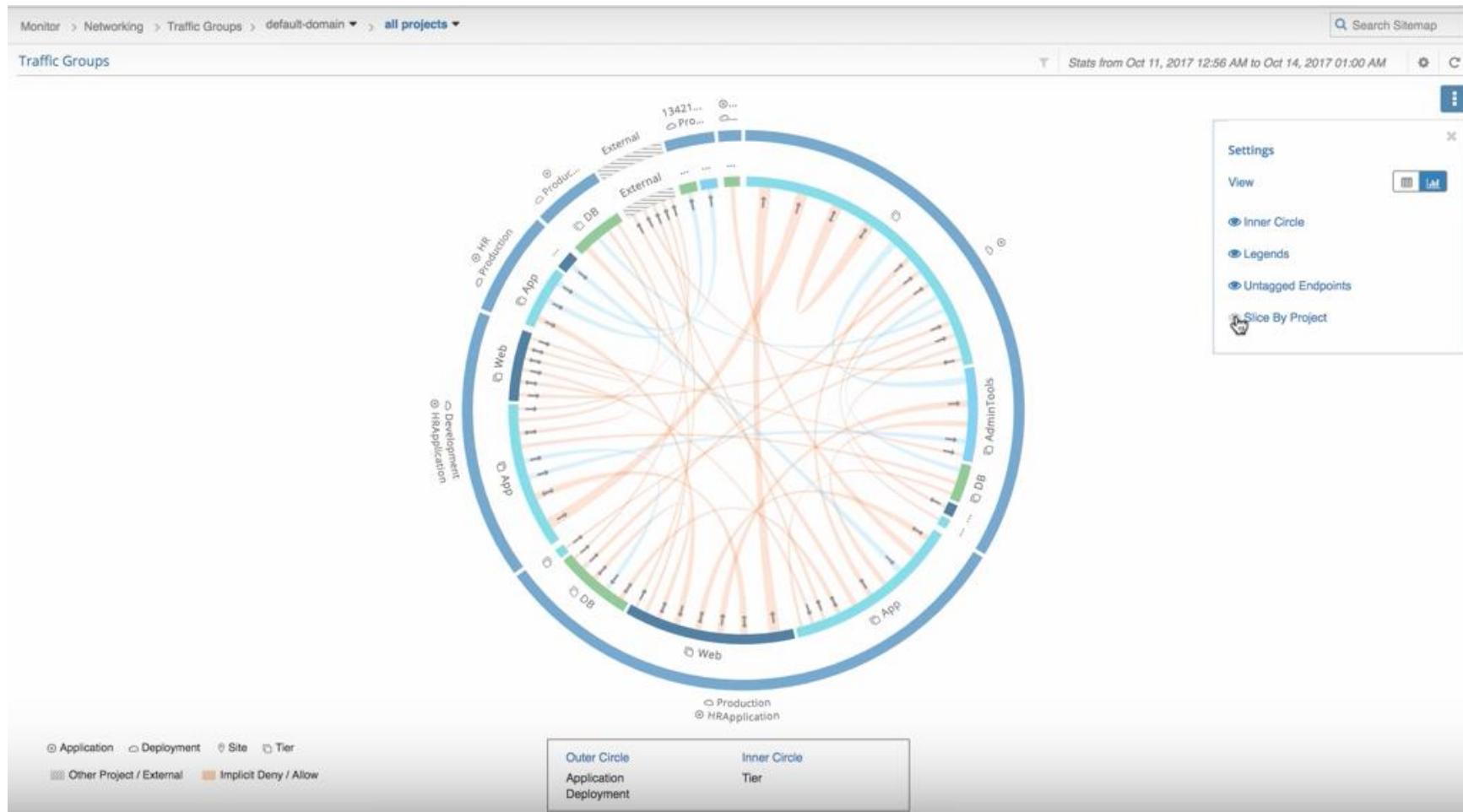
Objects at different levels can be tagged

Tags can be defined at different levels

- Global
- Project
- Network
- VM / Container / BMS
- Interface

Policies will finally be enforced at the interface level

VISUALIZATION



POLICY & FLOW VISUALIZATION

Monitor > Networking > Traffic Groups > default-domain > [all projects](#) Search Sitemap

Traffic Groups

All > [HRApplication](#)-[Production](#)-[App](#)
[Production](#)-[DB](#)

Select Endpoint

[HRApplication](#)-[Production](#)-[App](#) [Production](#)-[DB](#)

[Client Sessions](#) [Server Sessions](#)

Protocol (Server Port)	In Bytes	Out Bytes
TCP (443)	356.59 MB	362.47 MB
TCP (22)	382.46 MB	378.59 MB
TCP (8080)	434.13 MB	438.46 MB
ICMP (8080)	392.72 MB	390.34 MB
ICMP (22)	392.72 MB	390.34 MB
UDP (8080)	364.63 MB	359.57 MB
UDP (22)	431.26 MB	428.25 MB

Total: 7 records 50 Records

[Application](#) [Deployment](#) [Site](#) [Tier](#)

Stats for Last 12 Hrs More

[HRApplication](#)-[Production](#)-[App](#) \Rightarrow [Production](#)-[DB](#)

Matched Rules:

Policy: HRPolicy
Rule: 2a924d10-9de1-46a2-9632-b06e0265ddba

permit
global:tier=App \Rightarrow global:tier=DB

Service ApplicationTierCommunication

HRApplication - Production - App	Production - DB
Sessions Active Added	Sessions Active Added
Initiated: 0 0	Initiated: 0 0
Responded: 3 13	Responded: 0 0

Policy: Implicit Allow
Rule: 00000000-0000-0000-0000-000000000001

HRApplication - Production - App	Production - DB
Sessions Active Added	Sessions Active Added
Initiated: 0 0	Initiated: 0 0
Responded: 6 1	Responded: 0 0

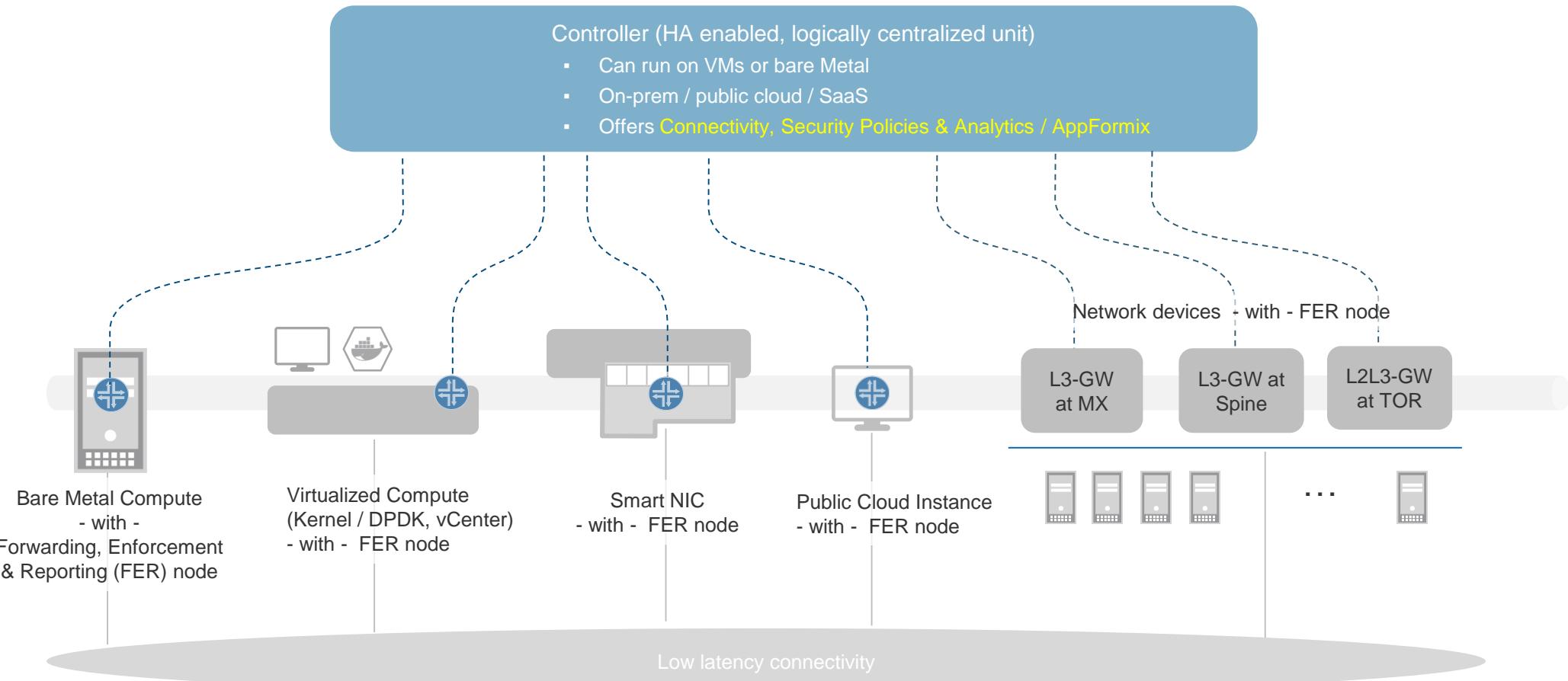
MULTIPLE ENFORCEMENT POINTS

Definition

Controller (HA enabled, logically centralized unit)

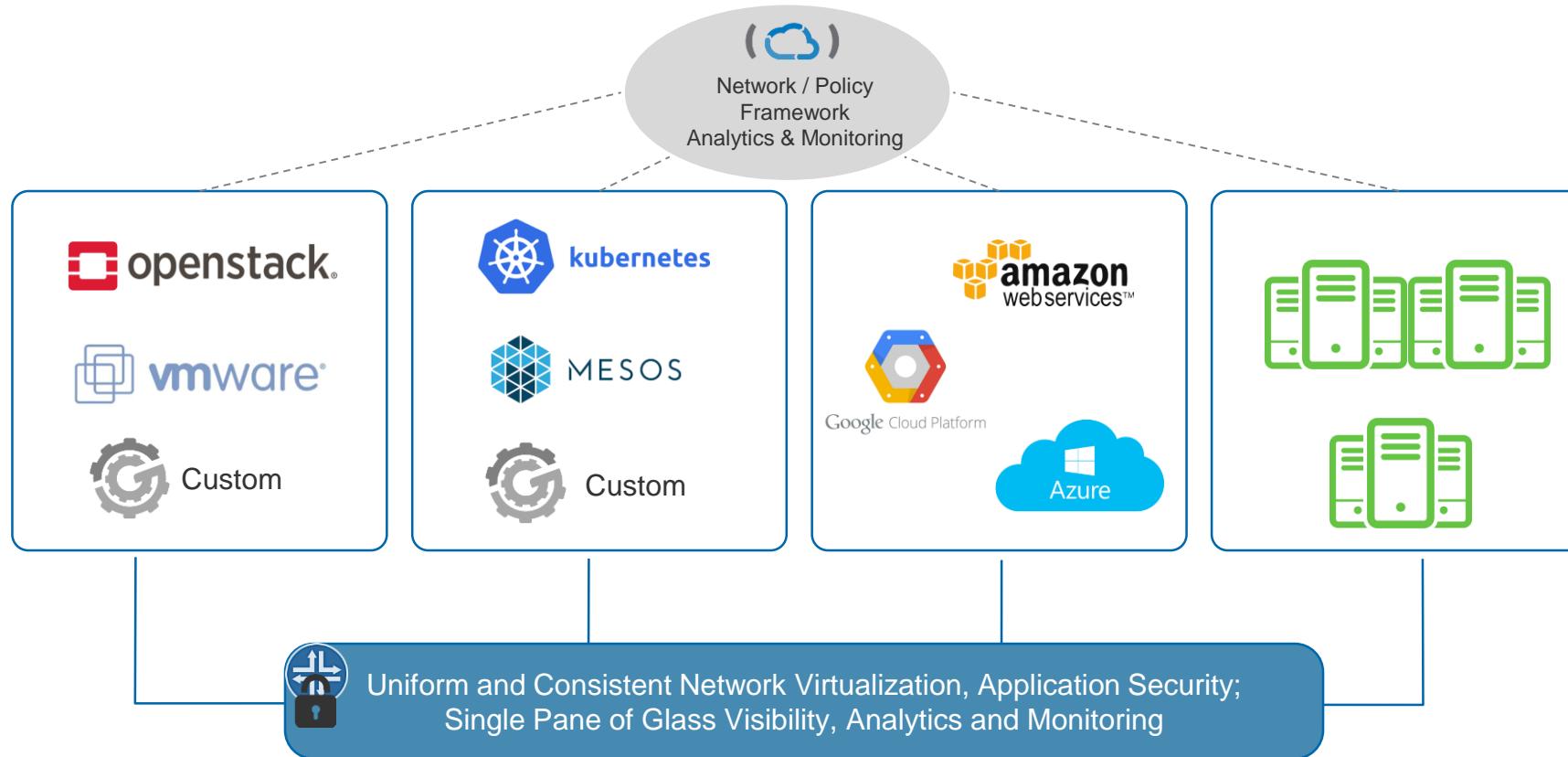
- Can run on VMs or bare Metal
- On-prem / public cloud / SaaS
- Offers **Connectivity, Security Policies & Analytics / AppFormix**

Enforcement

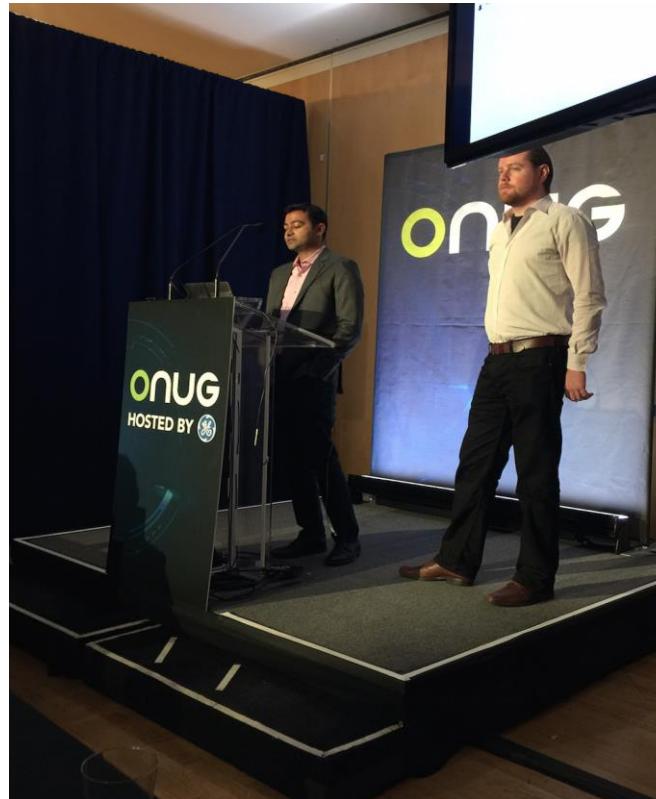


KEY TAKEAWAY

App Discovery, Tag based Policy & Visualization across heterogeneous and distributed environments
(ESXi & KVM VMs, K8s / containers, bare-metal servers, Public Cloud, etc.)



RECOGNITION AT 2017 ONUG



Blog: [Contrail Security wins 2017 ONUG Innovation Award!](#)

Q&A
