マルチクラウド / クラウドネイティブ時代におけるContrail Networkingの取り組み

2021/12/7

ジュニパーネットワークス株式会社

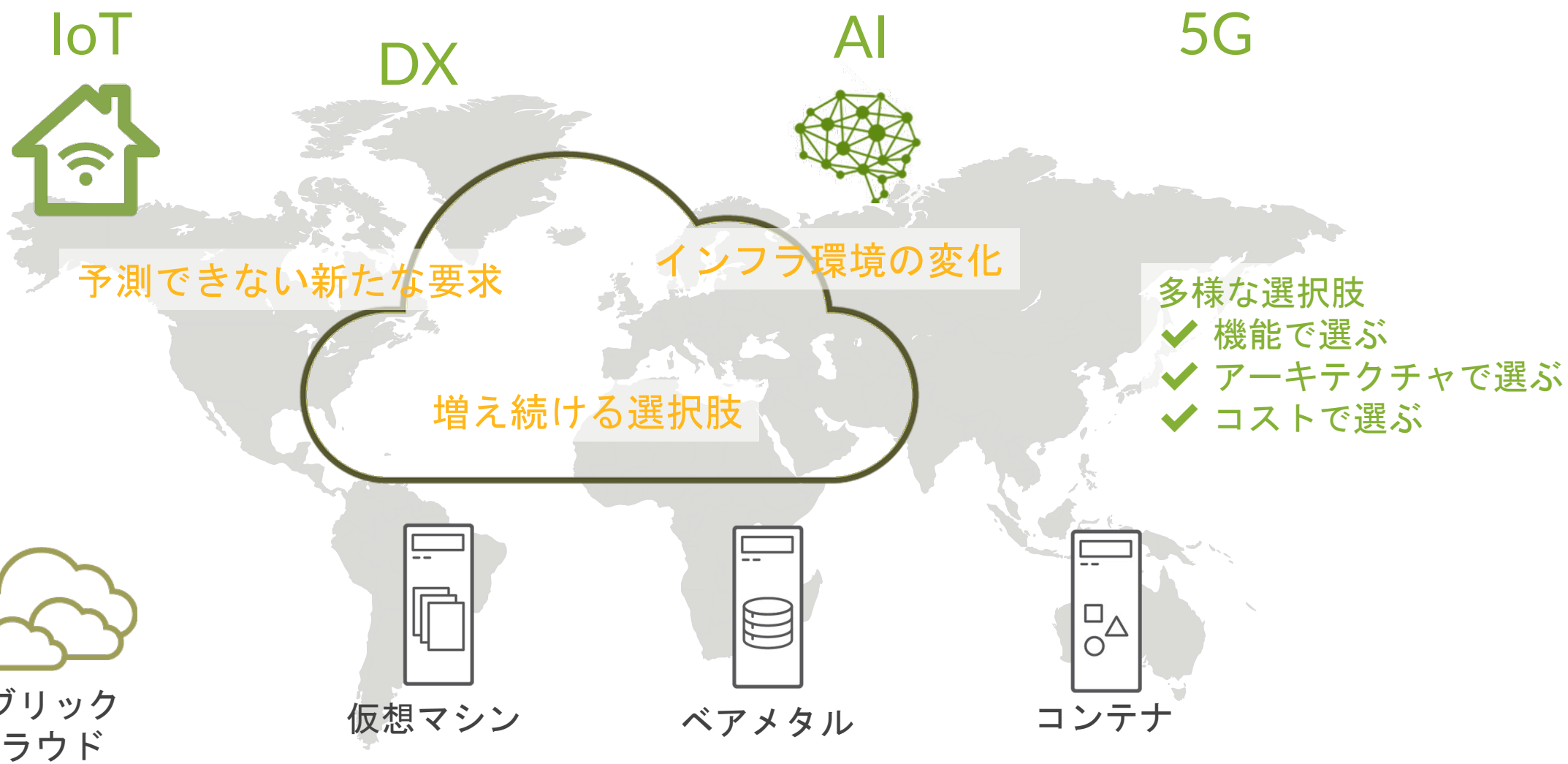
Agenda

- クラウドインフラのあるべき姿
- Contrail概要
  - Contrail Networking
  - Contrail Security
  - Contrail + OpenStack
  - Contrail + Kubernetes

Agenda

- クラウドインフラのあるべき姿
- Contrail概要
  - Contrail Networking
  - Contrail Security
  - Contrail + OpenStack
  - Contrail + Kubernetes

マルチ/ハイブリッドクラウド時代へ



マルチ/ハイブリッドクラウドのチャレンジ

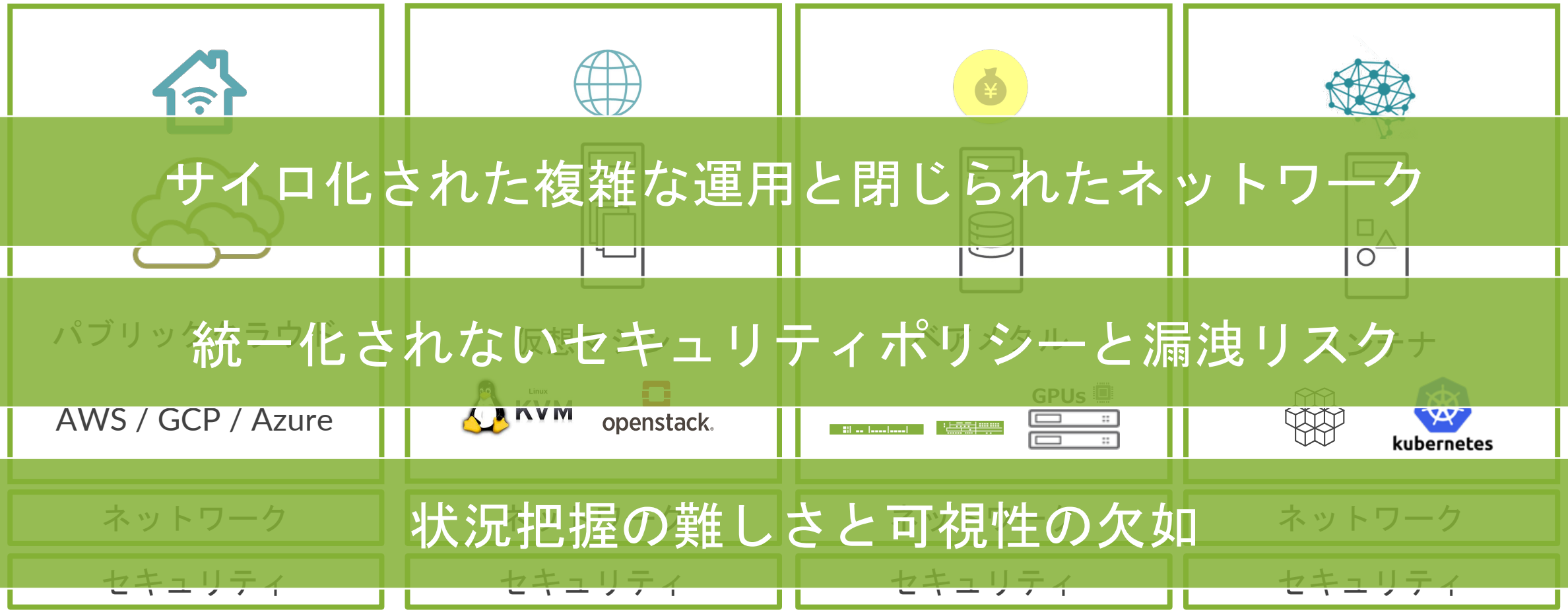
サイロ化されたインフラ

パブリッククラウド	仮想マシン	ベアメタル	コンテナ
AWS / GCP / Azure	Linux KVM, openstack.	GPUs	kubernetes
ネットワーク	ネットワーク	ネットワーク	ネットワーク
セキュリティ	セキュリティ	セキュリティ	セキュリティ

それぞれのインフラにそれぞれの異なるツールでそれぞれの管理者

マルチ/ハイブリッドクラウドのチャレンジ

サイロ化されたインフラ



サイロ化された複雑な運用と閉じられたネットワーク

統一化されないセキュリティポリシーと漏洩リスク

状況把握の難しさと可視性の欠如

それぞれのインフラにそれぞれの異なるツールでそれぞれの管理者

マルチ/ハイブリッドクラウドのあるべき姿

Any Cloud

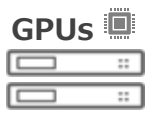
Any Workload

パブリッククラウド

AWS / GCP / Azure

仮想マシン

ベアメタル



コンテナ

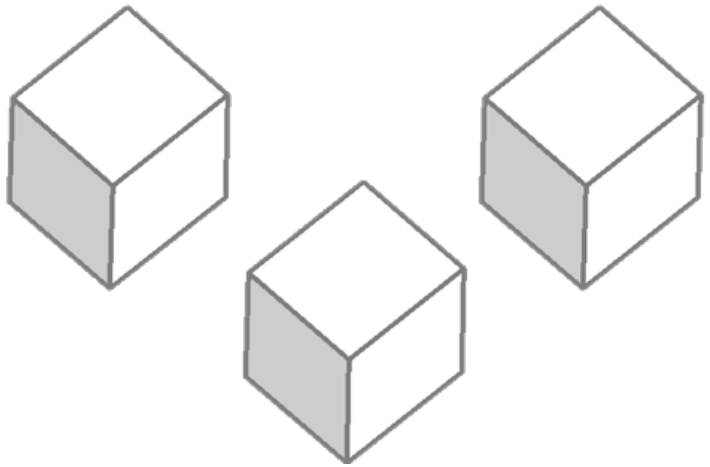
共通のネットワーク

共通のセキュリティ

クラウドネイティブ時代へ

旧Architecture

アプリケーション間接続：少



API Call : 少

microservices

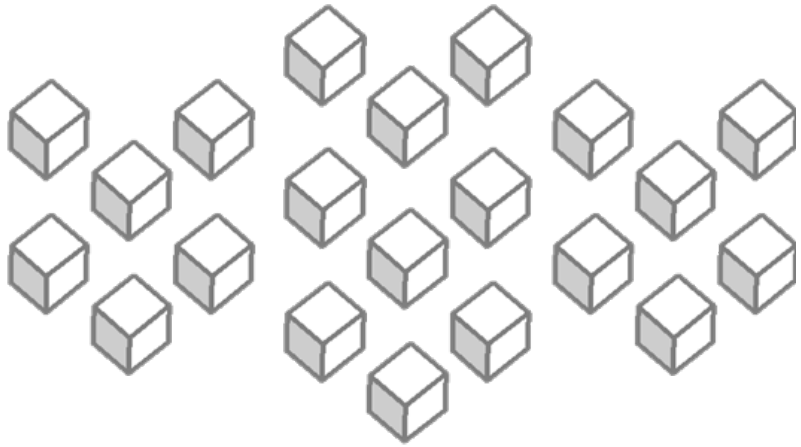
=

More

NETWORK

microservices

アプリケーション間接続：多



API Call : 多

ネットワークの重要度が増し、
多様な接続形態が求められる

KUBERNETESの進化

Today's Stack

Containers

VMs

VMware / RedHat / NUTANIX

Metal, private IaaS or public IaaS

Kubernetes
is eating
the Cloud!

Tomorrow's Stack

Containers + VMs

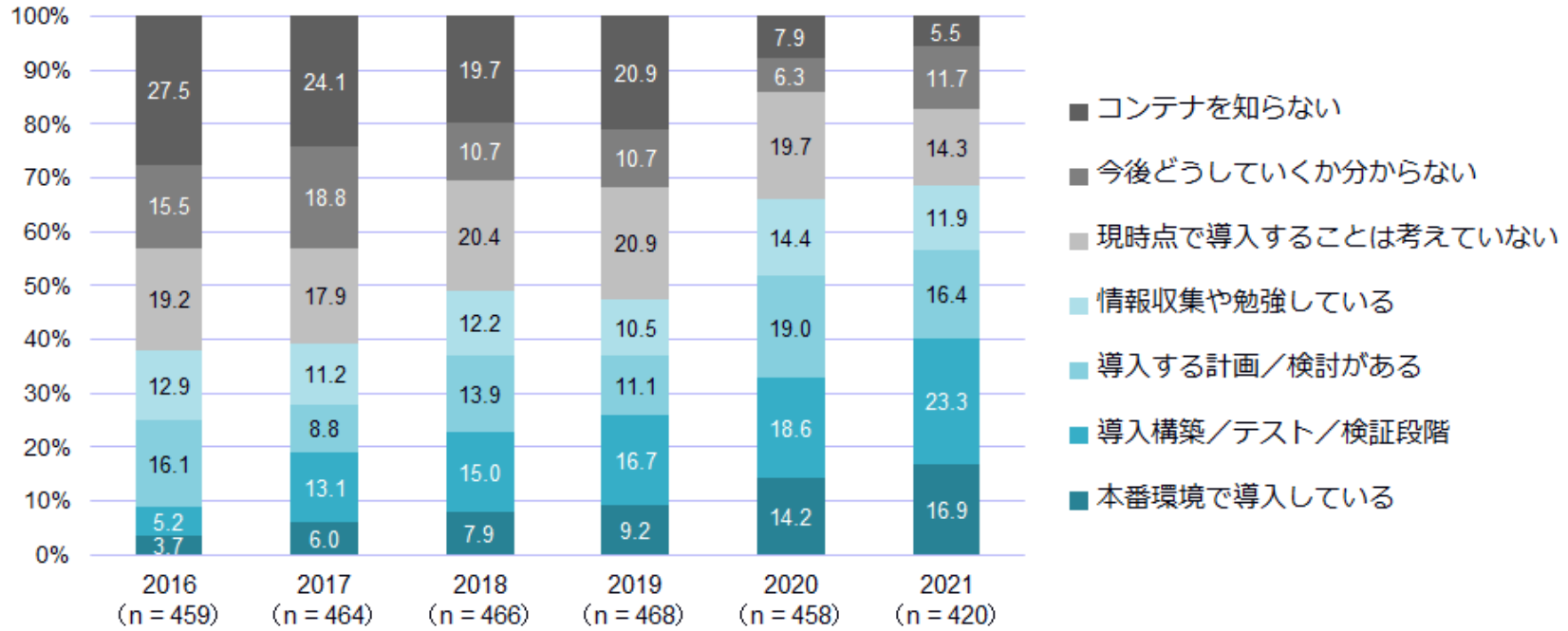
Many K8s distros + VMware / RedHat / NUTANIX

includes KubeVirt

Kubernetes on metal or public IaaS

K8S 国内導入状況 – IDC Japan Report

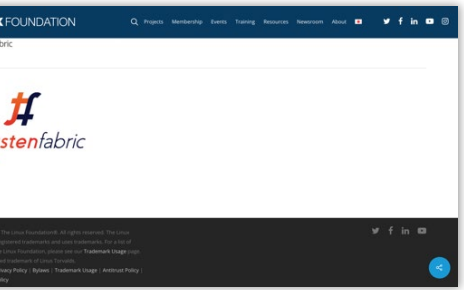
国内はコンテナの本格的な普及期へ



本番環境で使用している企業は16.9％となり、2020年調査から2.7ポイント上昇しました。さらに導入構築／テスト／検証段階にある企業は23.3％となり、2020年調査から4.7ポイント上昇しました。この2つを合わせた40.2％の企業がコンテナの導入を進めていることになり、国内はコンテナの本格的な普及期に入りました。これまではITサービス企業がコンテナの導入を牽引してきましたが、2021年調査ではサービス業、金融、製造など幅広い業種での導入が進んでいることが分かりました。様々な企業がDX（デジタルトランスフォーメーション）を進めていく中でアプリケーションのクラウドネイティブ化に取り組んでおり、コンテナ環境はその基盤としての採用が急速に進んでいます。

CONTRAILの進化

ContrailはOpenStackベースのアーキテクチャから
クラウドネイティブアーキテクチャへ進化



Linux Fundationへ寄贈

Juniperによる買収

OpenStackベースアーキテクチャ

2012

contrail systems

2013

Open Contrail

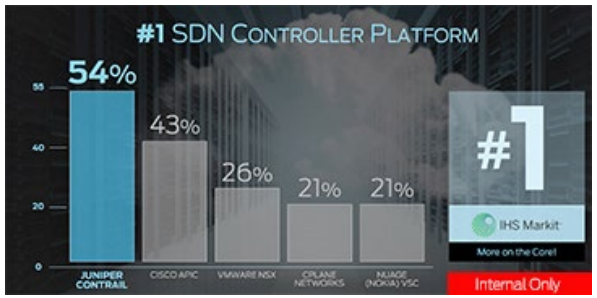
2018

Tungsten Fabric

2021

CN2

クラウドネイティブアーキテクチャ



OpenStack環境のNo.1 SDN Controller

Contrail
Enterprise
Multicloud

Underlay/Overlay/Security管理を含む
統合プラットフォーム

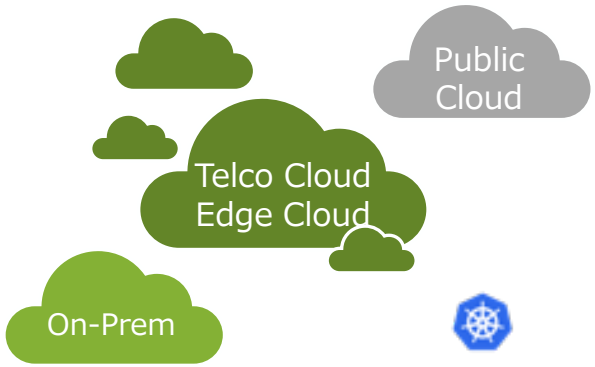
Agenda

- クラウドインフラのあるべき姿
- Contrail概要
  - Contrail Networking
  - Contrail Security
  - Contrail + OpenStack
  - Contrail + Kubernetes

Contrail Networking – 4つの柱

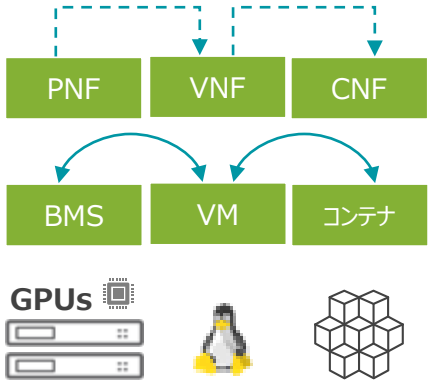
様々なユースケース・アプリケーションの変化に対応できるオープンでフレキシブルなCloudを実現

ANY CLOUD



オンプレミスMEC
Edge Cloud/Telco Cloud
Public Cloud

ANY WORKLOAD



BMS, VM, コンテナ
PNF, VNF, CNF

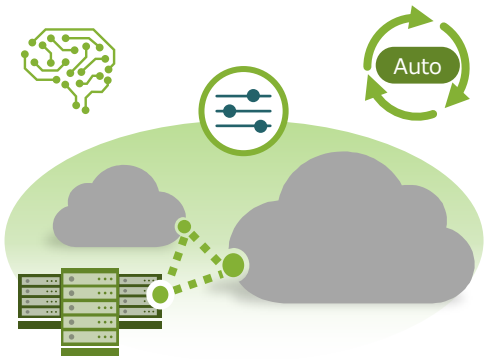
ANY DEPLOYMENT

OpenShift / Kubernetes /
OpenStack / KVM

VMware / RedHat / Canonical

OpenShift, OpenStack,
K8s

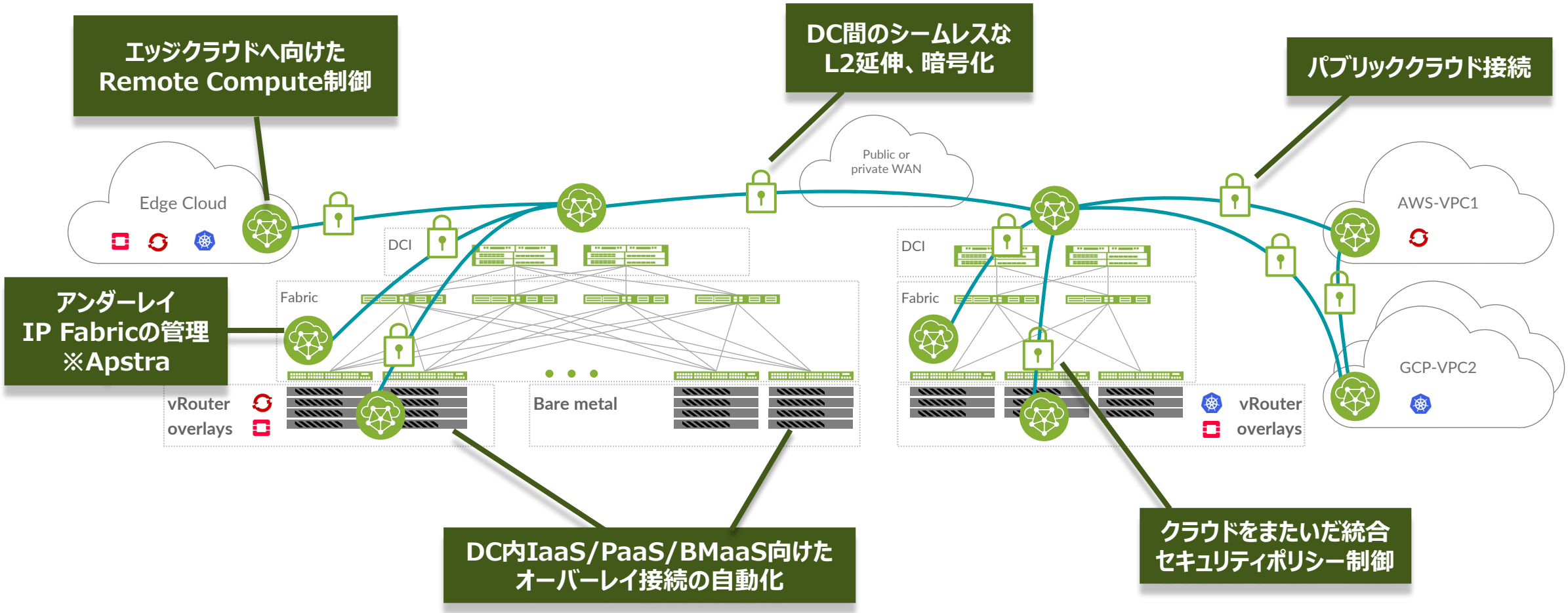
AUTOMATON



設定・構築自動化
クローズドループ
インテリジェンス

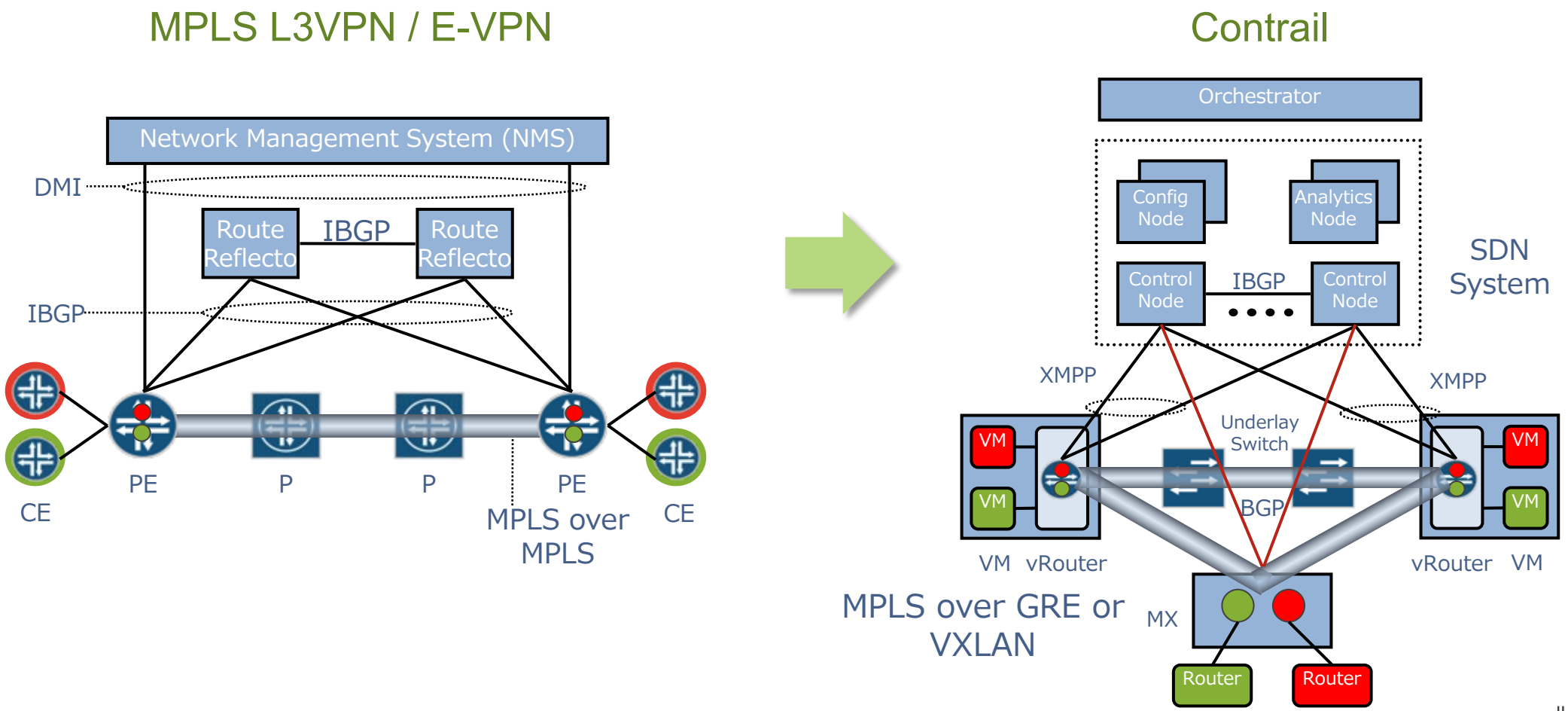
マルチ/ハイブリッドクラウドにおけるEnd-to-END制御

クラウドのワークロードにおけるロケーション・ダイバーシティが進むことでネットワークやセキュリティの重要度が増してきている



CONTRAIL アーキテクチャ

MPLS/L3VPNベースのアーキテクチャを採用し、Computeリソース外へのシームレスな接続



CONTRAIL NETWORKING

ネットワーク仮想化の課題

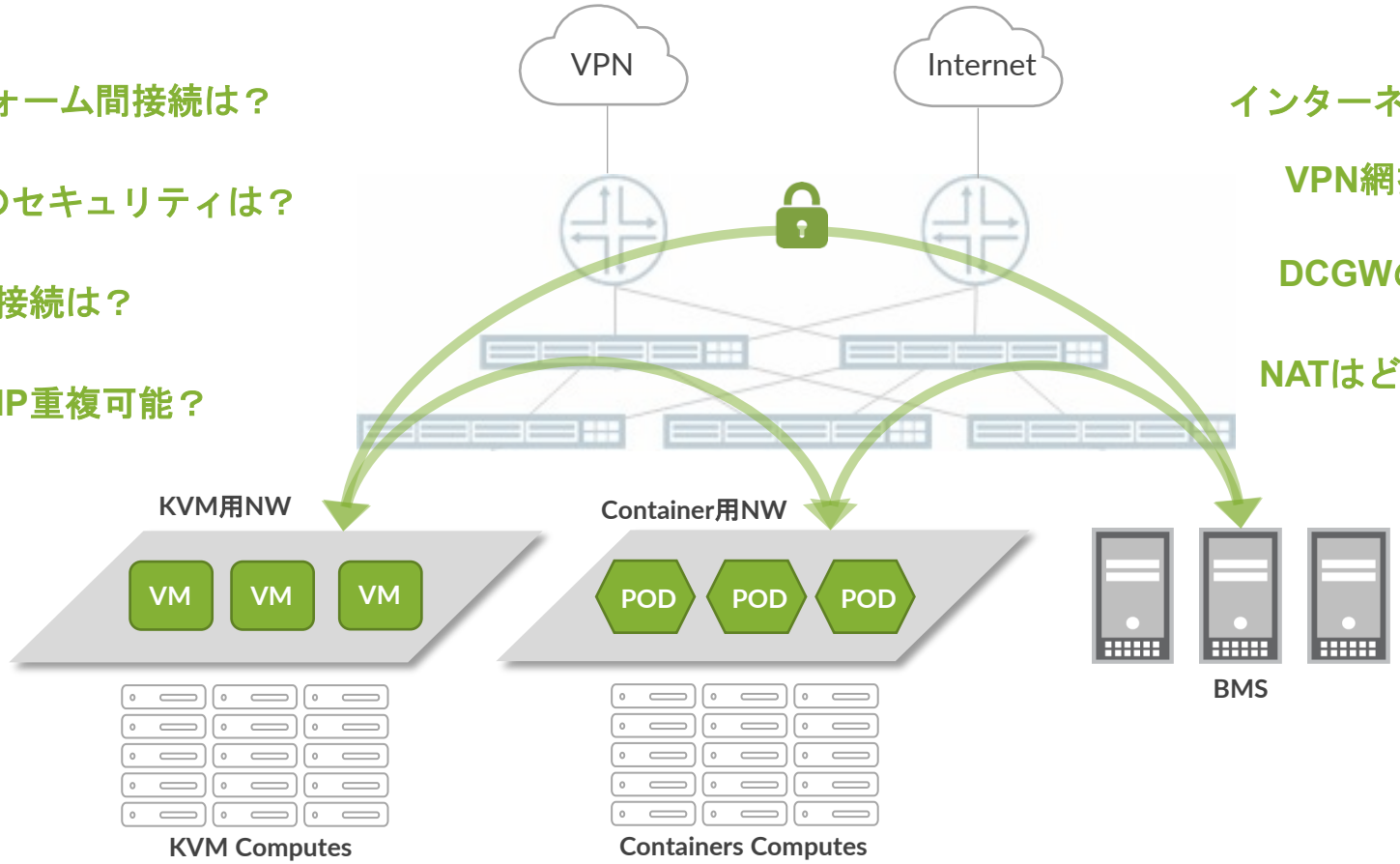
- 多様化するアプリケーションニーズに答えるため、VirtualMachine, Container, Baremetal Serverなど、プラットフォームを自由に選択できるインフラ基盤が求められる中、ネットワークはサイロ化されたまま

プラットフォーム間接続は？

プラットフォーム間のセキュリティは？

テナント間接続は？

IP重複可能？



インターネット接続は？

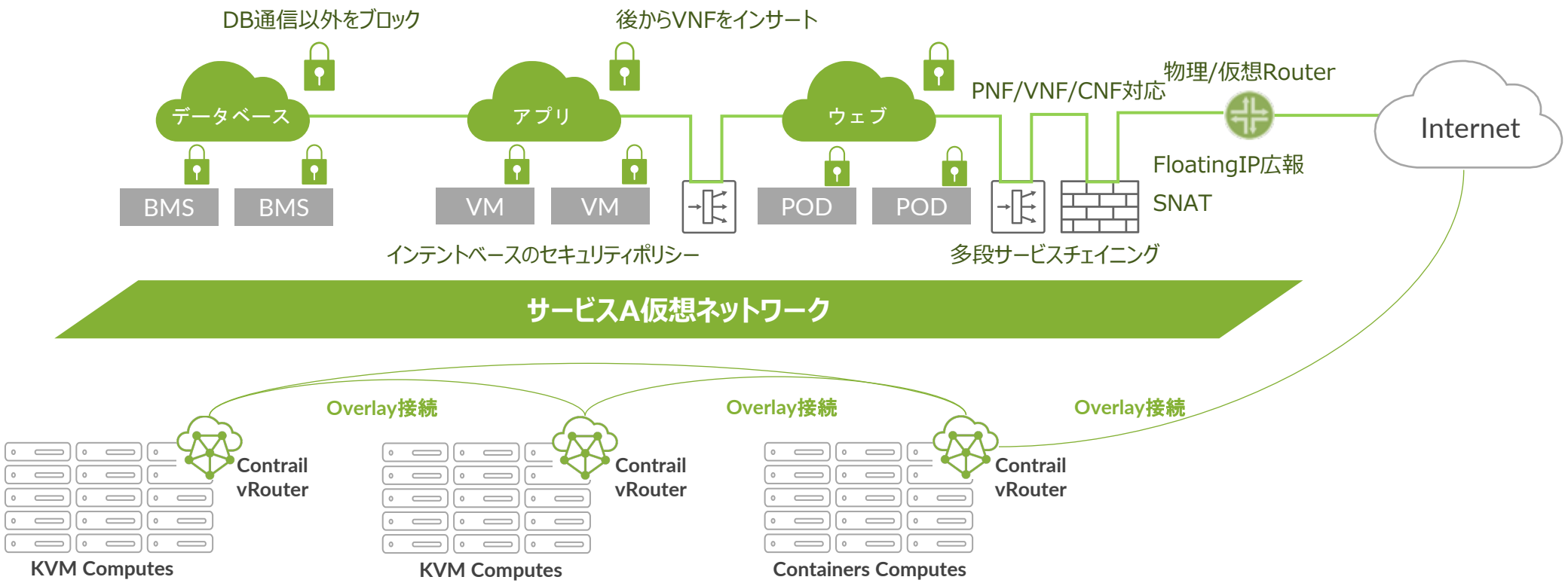
VPN網接続は？

DCGWの管理は？

NATはどこで実施する？

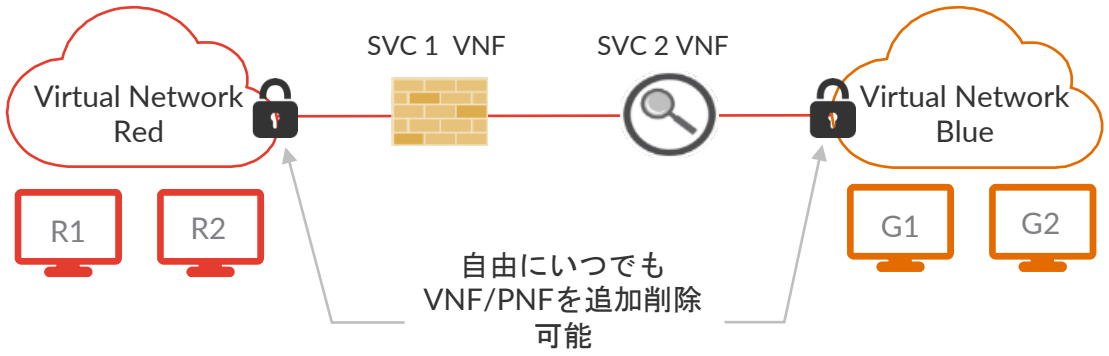
Contrailの仮想ネットワーク

- Contrail vRouterによるプラットフォームを跨った共通のネットワーク＆セキュリティポリシー
- IPベースのフィルタリングではなく、サービスにタグ付けしたインテントベースのセキュリティポリシー

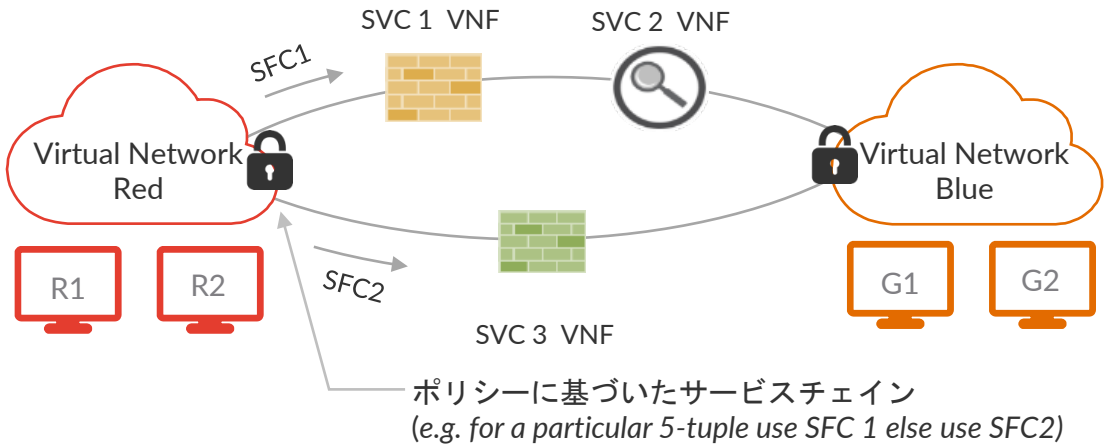


多様なサービスチェイニング

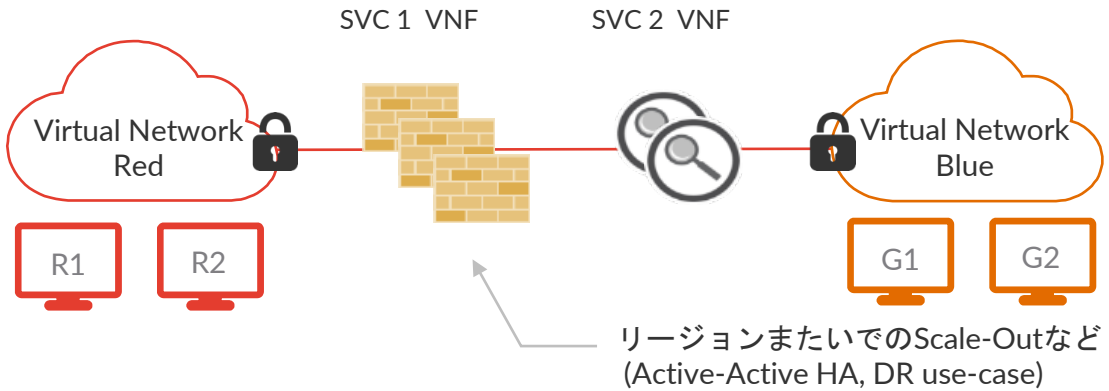
多段サービスチェニング（PNF, VNF, CNF）



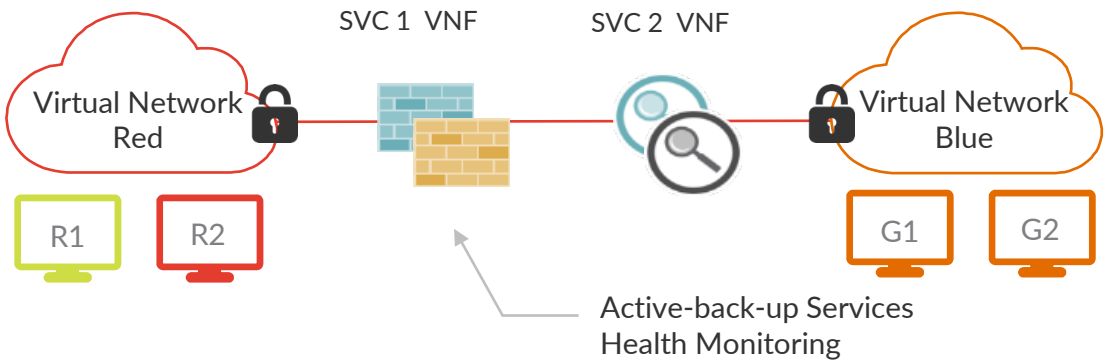
ポリシーベース・サービスチェイニング



スケール・アウト／スケール・イン (Active-Active HA)

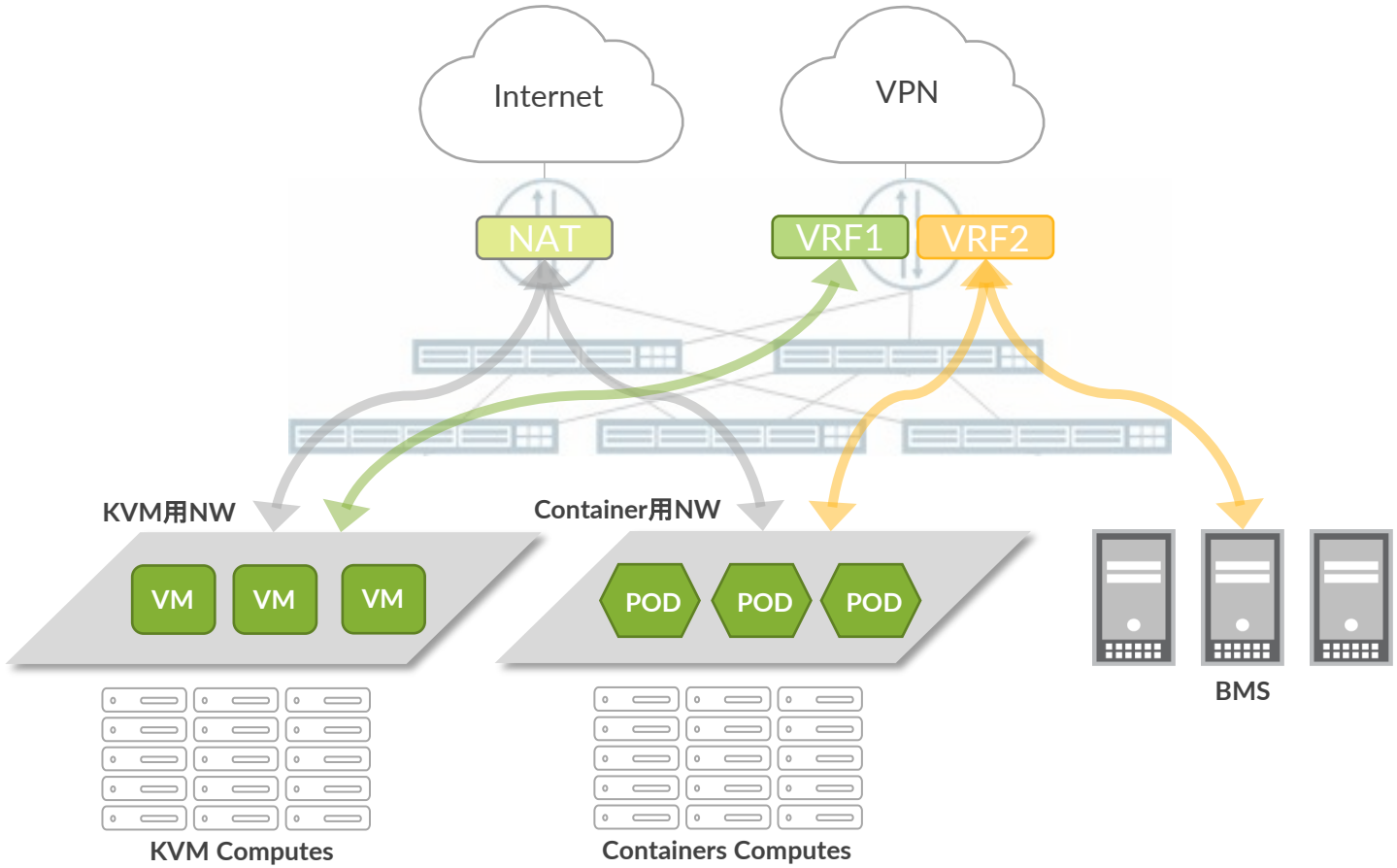


アクティブ・スタンバイ



DCGW接続

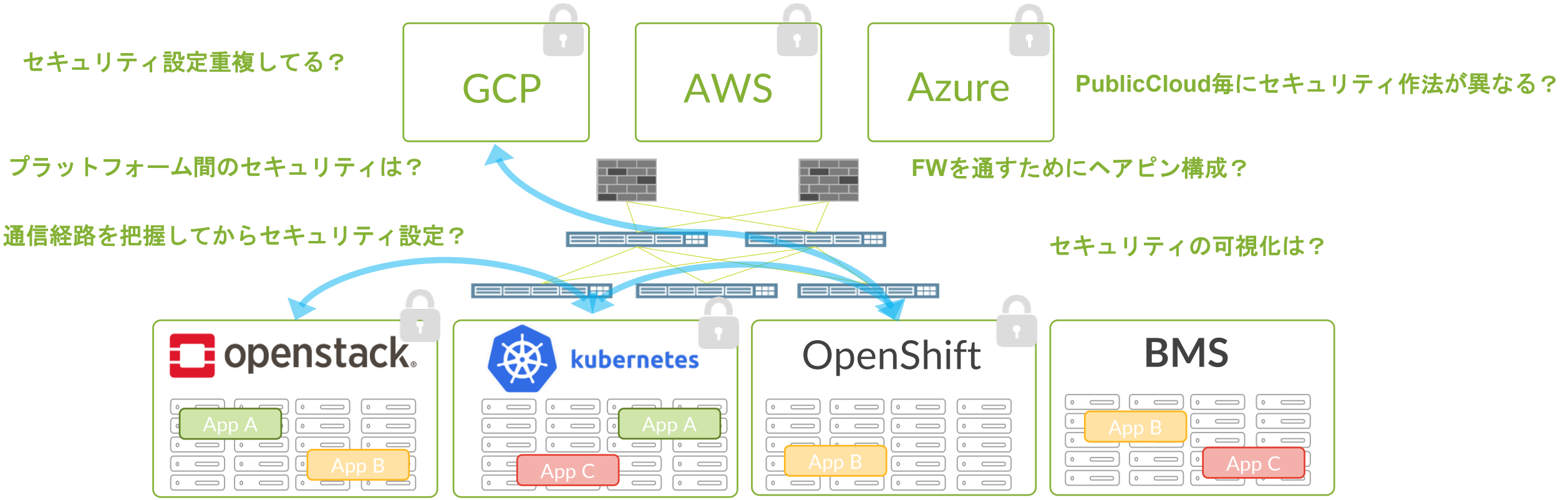
- 仮想ネットワークの外部接続には物理ルータを使用可能となり、ソフトウェアGWのボトルネックを解消
- 仮想ネットワークのVPN網への延伸、NATによるInternet接続が可能



CONTRAIL SECURITY

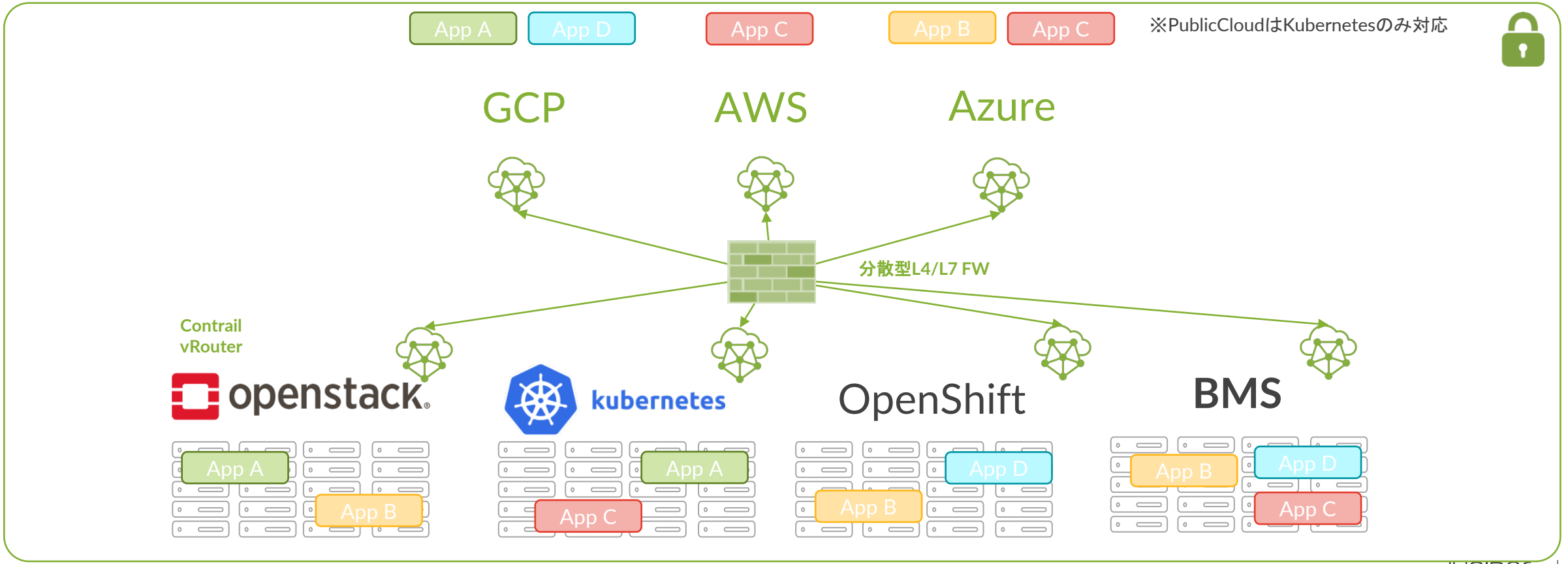
仮想ネットワークのセキュリティ課題

- セキュリティはプラットフォームやクラウド単位で実施されており、一貫したセキュリティが担保されていない
- アプリへの動的なIP付与が一般化され、IPベースのセキュリティ設定は困難に
- Internetや外部ネットワークとの境界に設置するFWだけでは脅威を防ぎきれない



Contrailの分散型FW

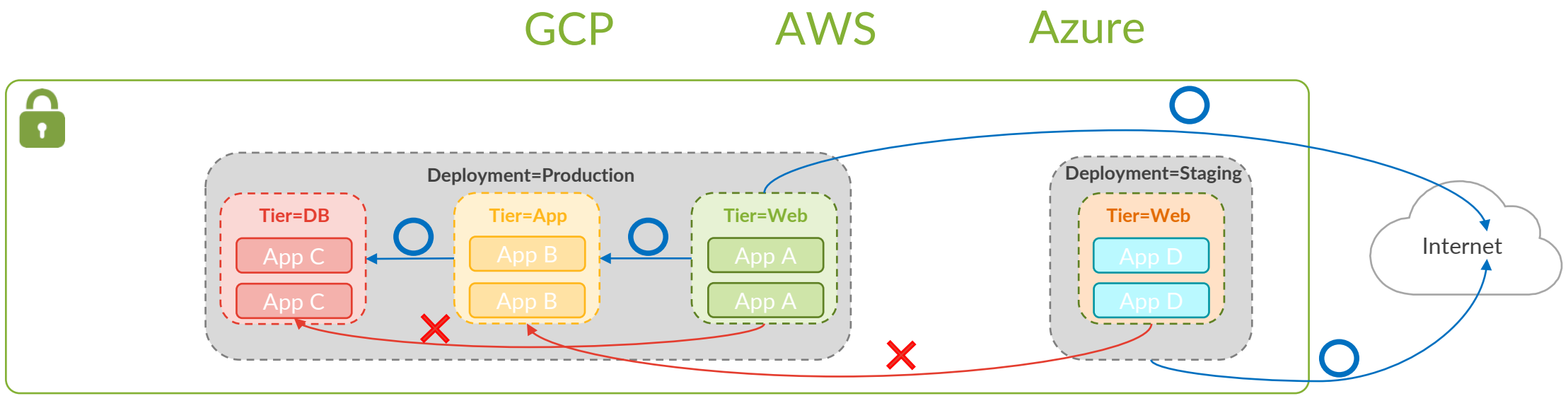
- 各プラットフォームにデプロイされたContrail vRouter Agentが分散型L4/L7 FWとして稼働し、仮想NW全体でセキュリティポリシーを担保
- 分散型FWによりロケーション、プラットフォームに捉われずにセキュリティ設定可能



Contrail Security

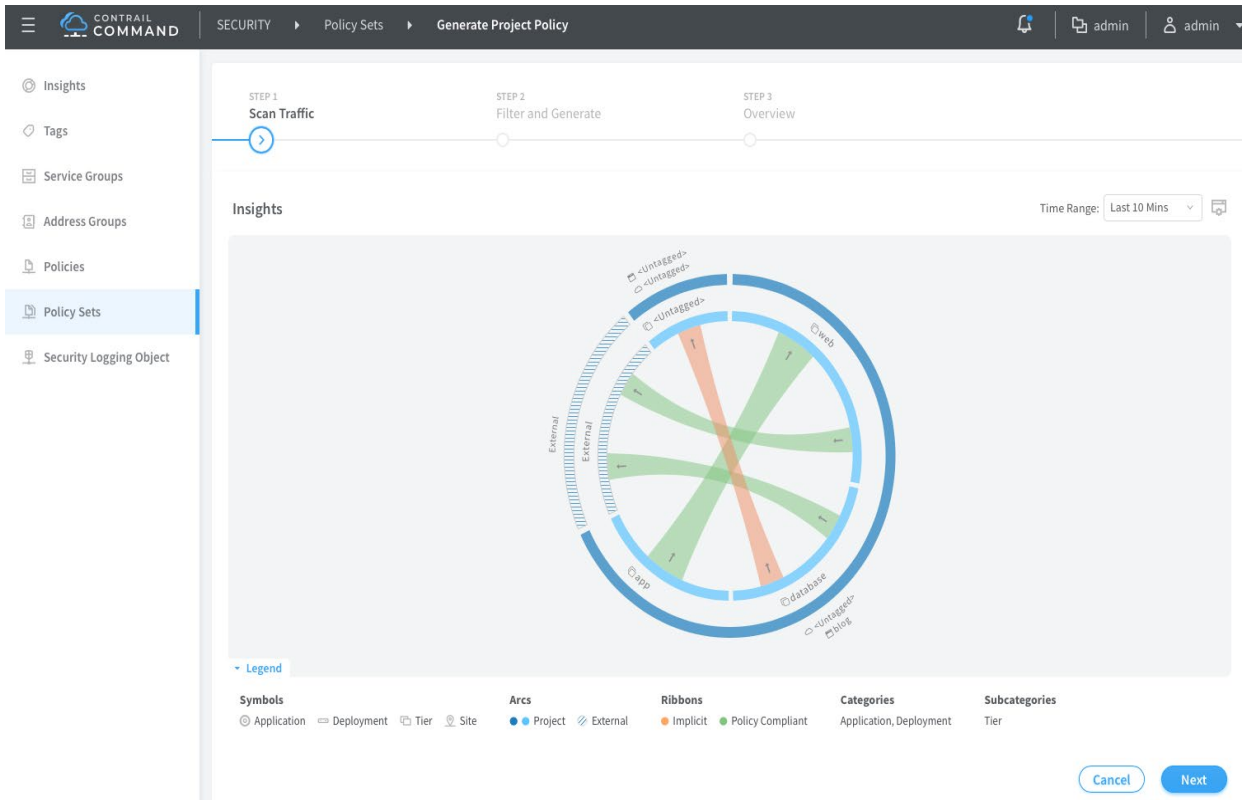
- 分散配置されていたアプリケーションを用途毎にグループ化しタグ付け
- IPベースではなく、インテントベースのフィルタリング
- セキュリティポシリーの一括適用

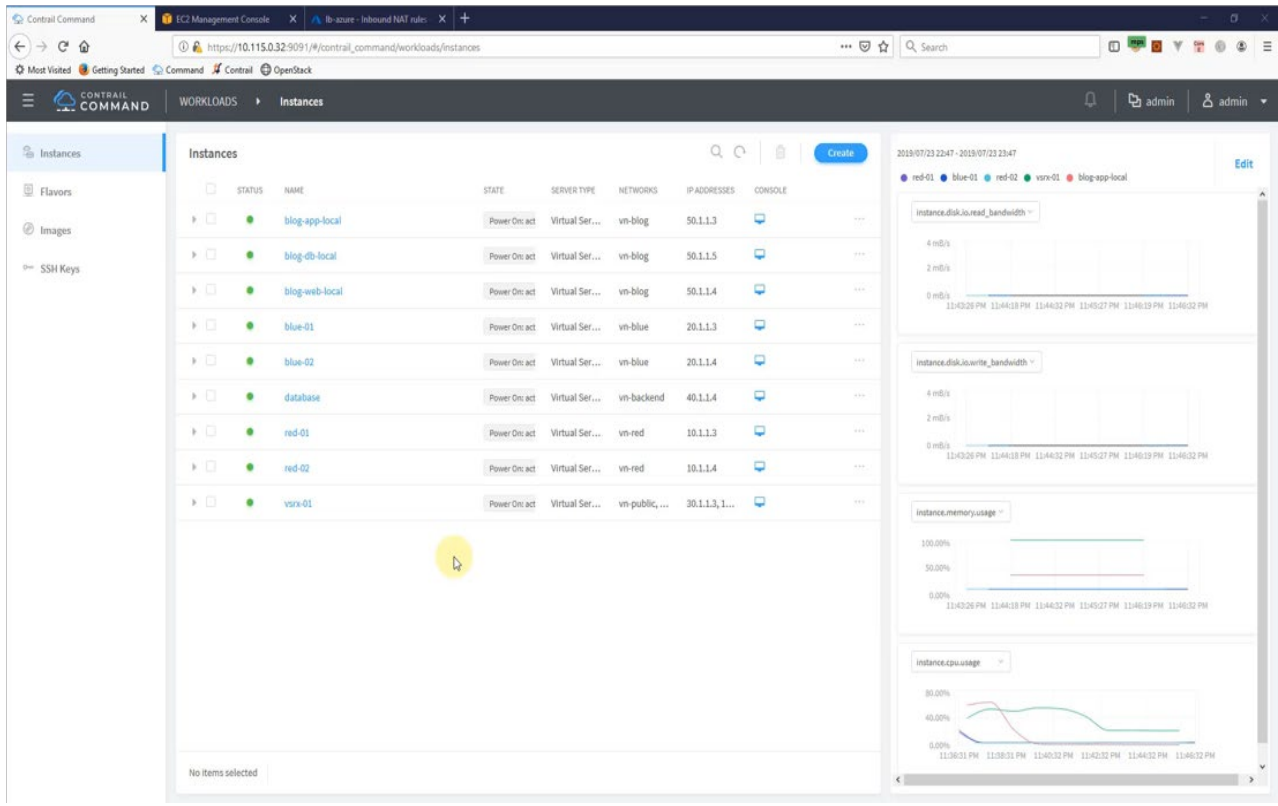
Allow TCP 3036 tier=app > tier=db match Deployment=Production
Allow TCP 80 tier=web > tier=app match Deployment=Production
Deny TCP 80 tier=web > tier=app match Deployment=Staging



Contrail Security GUI

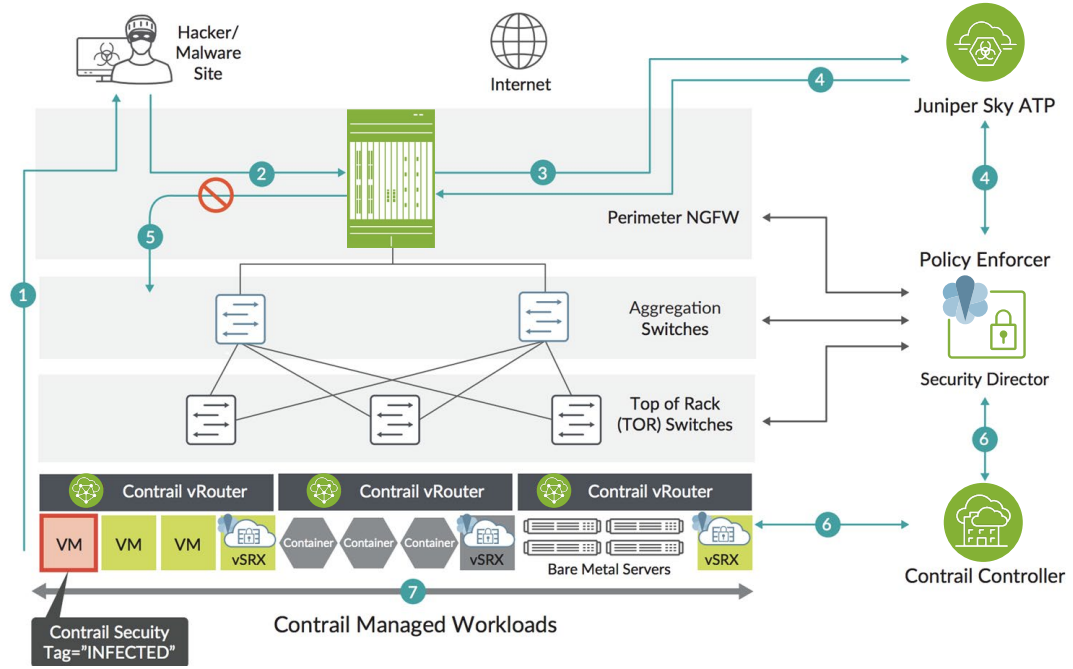
- トラヒックフローの見える化
- タグ付けされたアプリのトラヒックをモニター分析し、必要なセキュリティポシリーを設定可能
- セキュリティポリシー毎のトラヒック流量把握
- 容易なセキュリティポリシーの有効・無効化





脅威インテリジェンスとContrailによる自動隔離連携

Contrail + Security Director Policy Enforcer + ATP



マイクロセグメンテーションを超えて

1. VMがマルウエアファイルのダウンロードを試みている、もしくはC&Cサーベへの接続を試みようとしている
2. vSRXでスキャンを実行
3. vSRXからATPもしくはSkyATPへファイルを送信
4. ATPがマルウエアかどうかを判断しポリシーエンフォーサへ通知
5. vSRX、Switchにて自動で隔離を実行

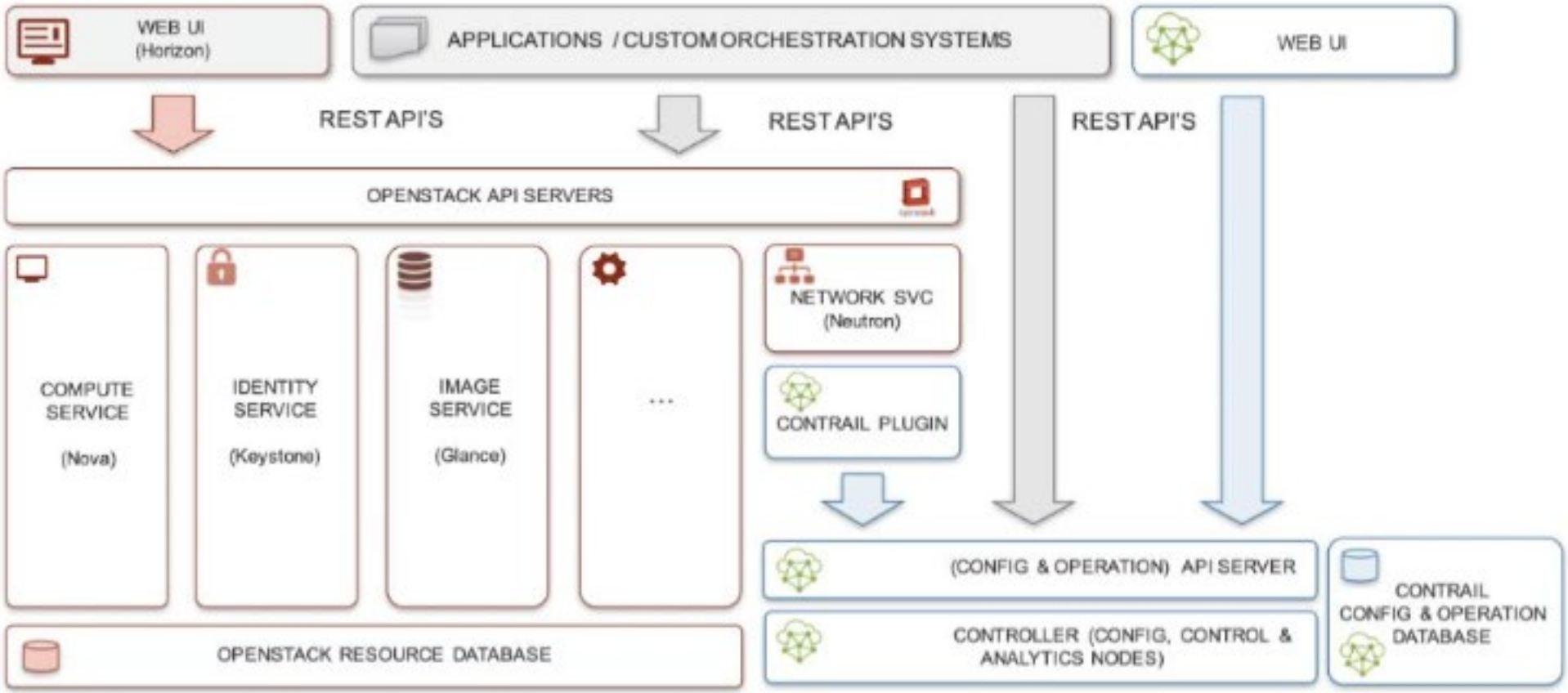
Integration with Contrail:

6. ポリシーエンフォーサがContrailへ適切なセキュリティ・タグを付けて隔離Security Groupへ隔離
7. セキュリティ管理者で事前に対応アクション定義や、さらなるアクションを定義

CONTRAIL + OPENSTACK

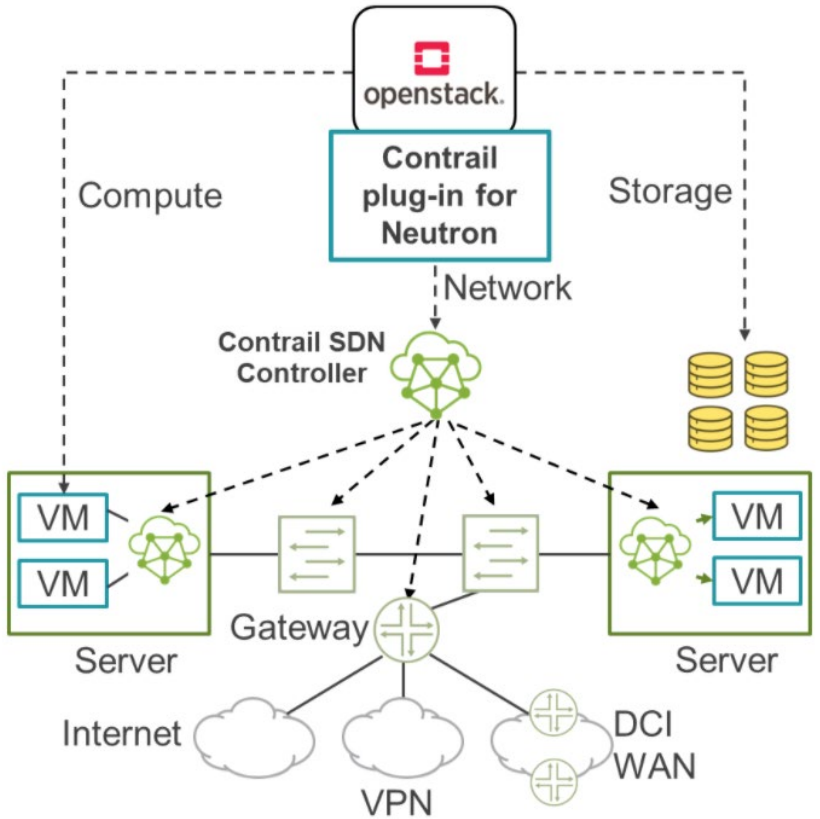
CONTRAIL + OPENSTACK

- ContrailはOpenStack Neutron Plugin
- OpenStack ネットワークのシンプル化、ハイパフォーマンス、ハイパースケール、多様なネットワーク機能



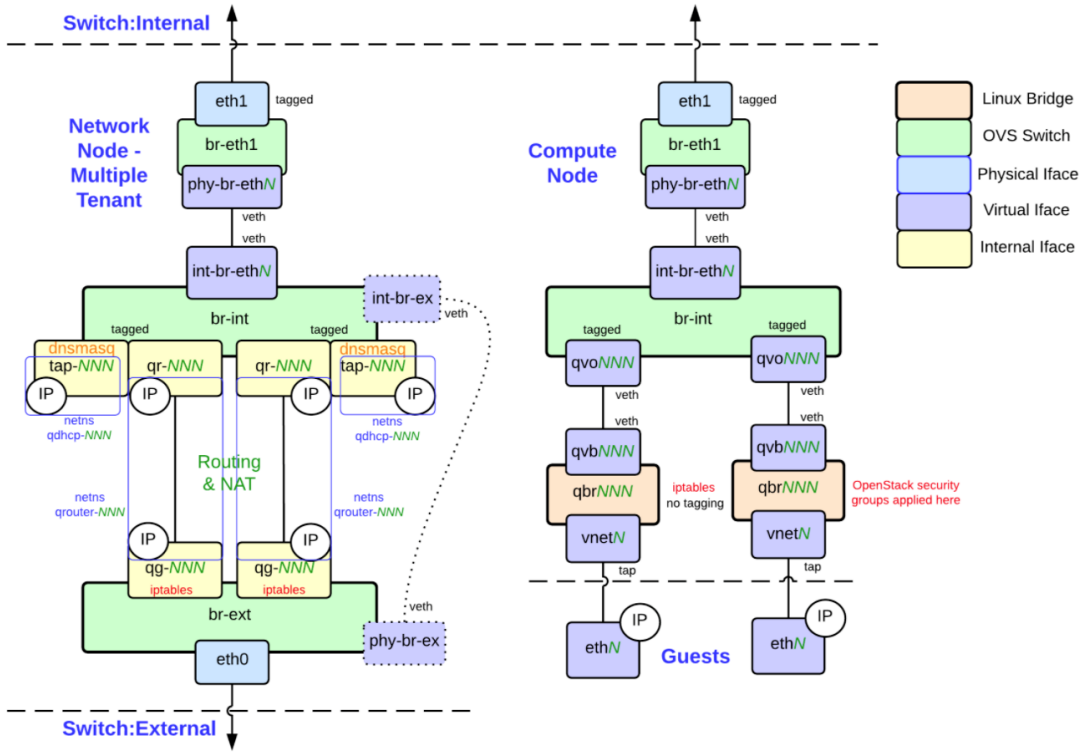
CONTRAIL + OPENSTACK

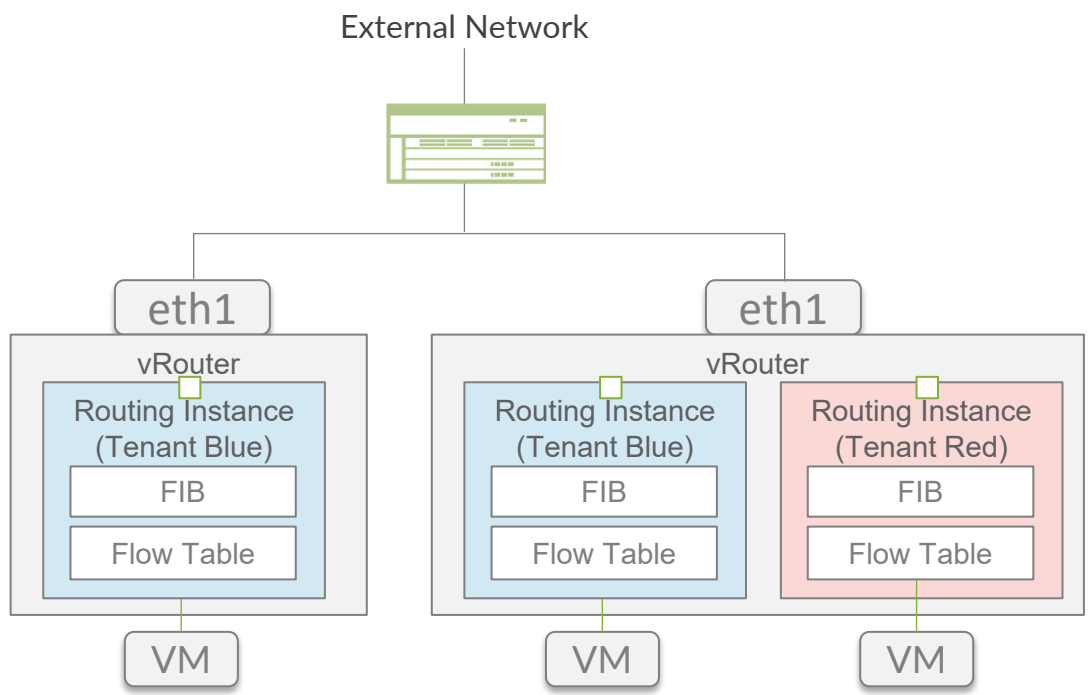
- OpenStackではSDN, non-SDN環境の選択が可能であるが、スケール、パフォーマンス、運用管理を考慮するとContrailのようなSDN化が必要である
- Contrail Neutron Pluginにより、VirtualNetwork, VirtualRouter, Firewall, LoadBalancerなどのネットワーク機能をContrail Controllerを介して管理が可能
- 同一ControllerからInternet/VPNなどの外部接続、PublicCloud接続、およびDCIなどNeutron標準では有していないネットワーク機能を実現



CONTRAIL + OPENSTACK : 内部構成のシンプル化

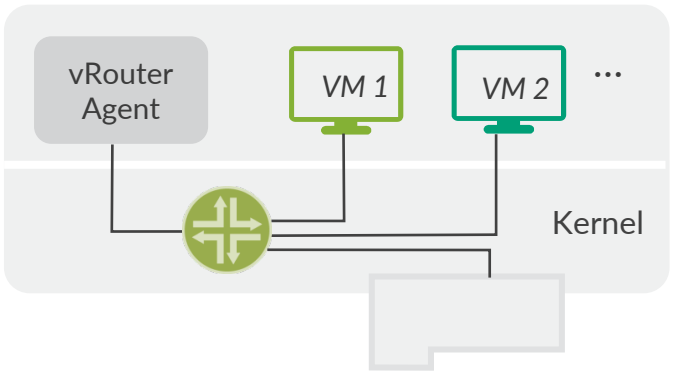
- OVSベースのOpenStackではLinuxBridge, OVS, TAPで複雑な内部構成となっている
- Contrail環境ではNetworkNode不要で、DHCP/Metadata/L3サービスをvRouterが担いシンプルな構成となる



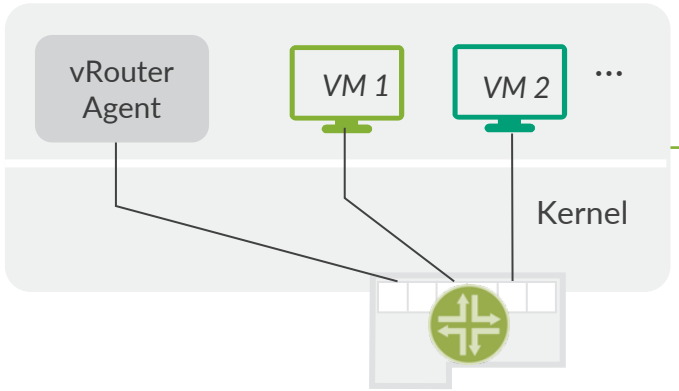


CONTRAIL + OPENSTACK : ハイパフォーマンス

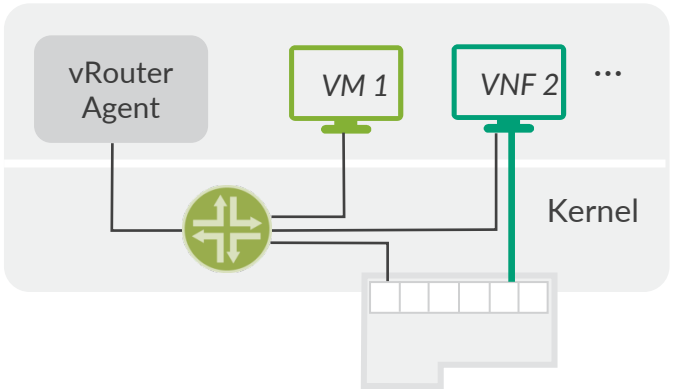
KERNEL VROUTER



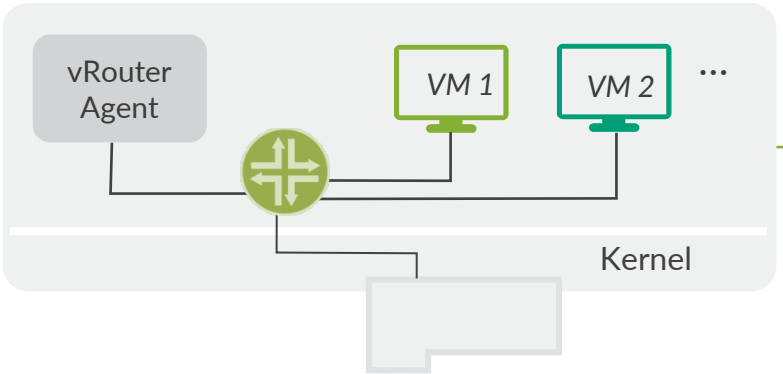
SMART NIC VROUTER

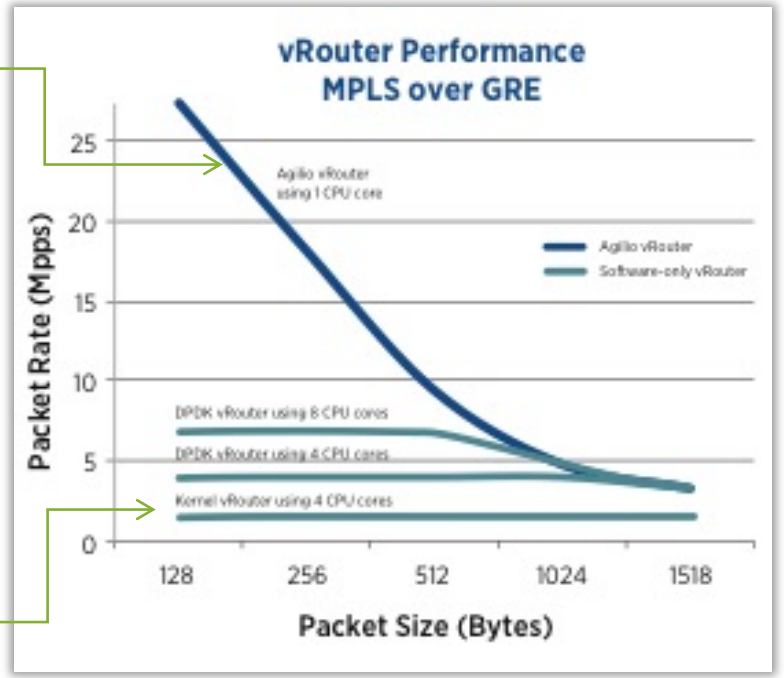


SR-IOV – VROUTER COEXISTENCE



DPDK VROUTER





Source:netronome
https://www.netronome.com/m/redactor_files/PB_Agilio_vRouter.pdf

CONTRAIL + KUBERNETES

KUBERNETES CNI

CNI: CNCFプロジェクトで管理されており、
Kubernetesで作成するPODにネットワークを提供

canal

flannel

Calico

weave net

Tungsten Fabric

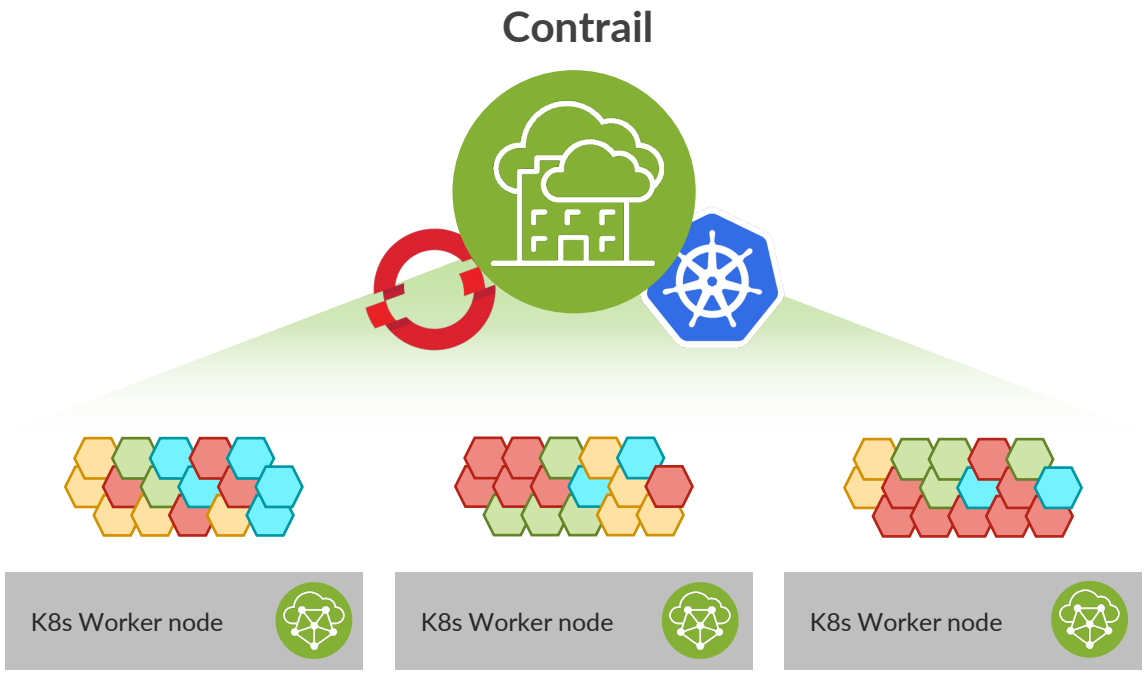
Contiv

. . .

どのCNIを選択するべきか？

実装モデル(Overlay, Underlay, Routing)、POD/リソースのL2/L3接続、NetworkPolicyサポート、ロードバランシングサポート、性能、運用管理など、ネットワーク要件に適したCNIを選択する必要がある

CONTRAIL + KUBERNETES



距離制限のないWorker Node間接続

マルチクラスタ / マルチワークロード

クラスタ外への接続 (GW RouterとのVPN/EVPN接続)

ハイパフォーマンス (DPDK, SR-IOV, SmartNIC)

K8S + Contrail

接続性

- Namespaces または Virtual Network(VRF)によるMultiTenancy
- IP/Subnetのオーバーラップ
- DNS, Service / Ingress load balancing サポート
- マルチクラスタ接続 (BGP)
- マルチインターフェース(with or without Multus)
- コンテナサービスチェインニング(Juniper cSRX containerized NGFW)
- POD/Service L2/L3接続
- BMS / VMとのL2/L3接続
- DualStack / IPv6 Only Overlayサポート
- GW Router接続 / GW Less Underlay接続
- DPDK/SR-IOV/SmartNIC対応

可視化

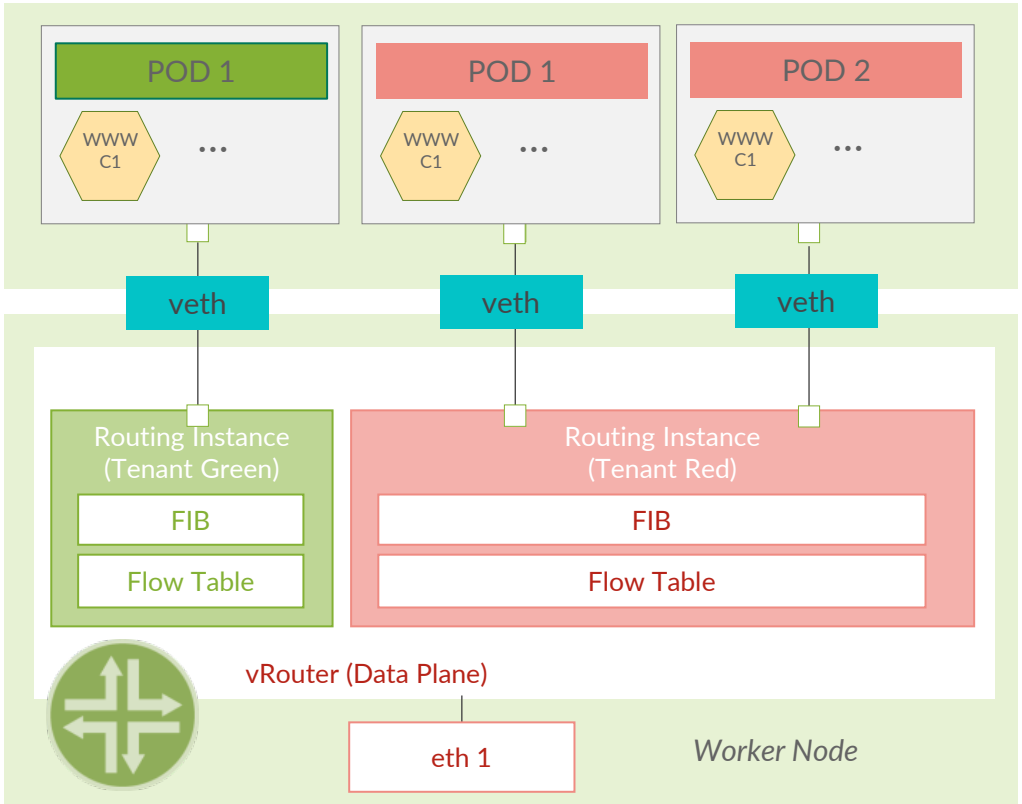
- ブロックされた脅威を含めNetwork Policyの可視化
- Traffic / Flow Monitorinig

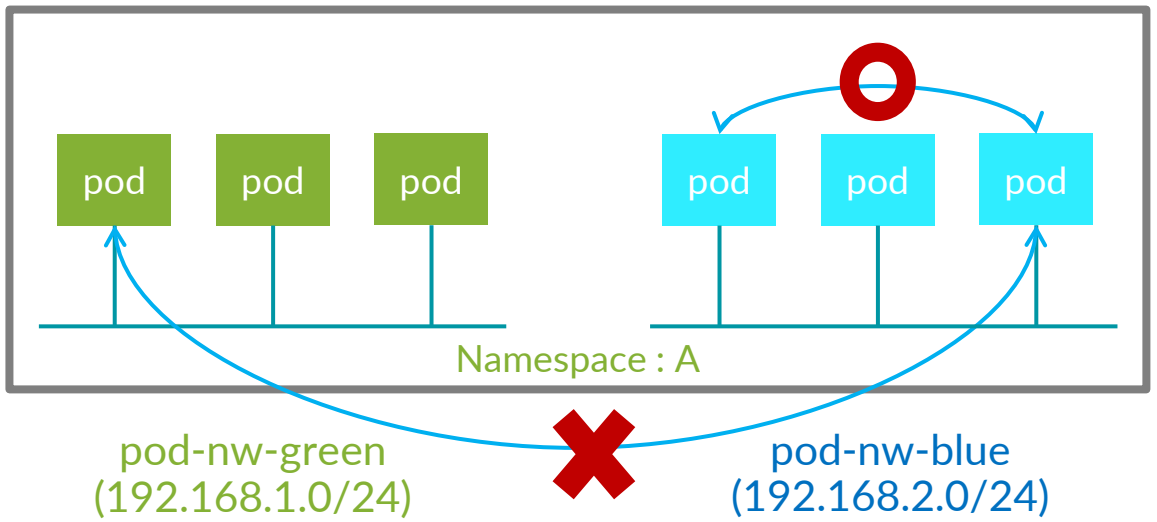
セキュリティ

- Network Policy & Contrail PolicyによるMicro Segmentation
- Tagベースセキュリティポリシー
- cSRXによるL7 FW

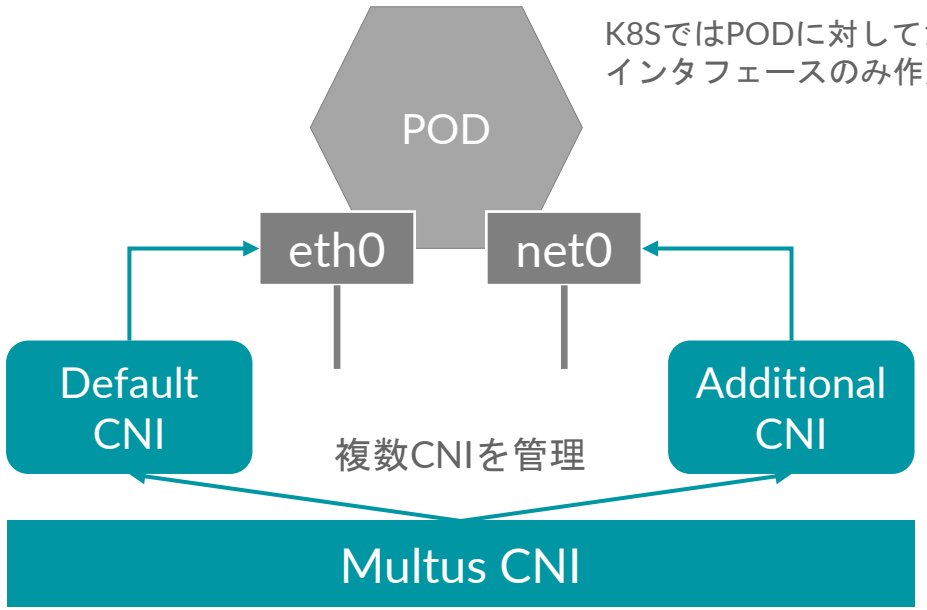
CONTRAIL + KUBERNETES : ネットワーク分離

- 仮想マシンネットワークのようにネットワークを分離
- マルチテナント、マルチインターフェース対応

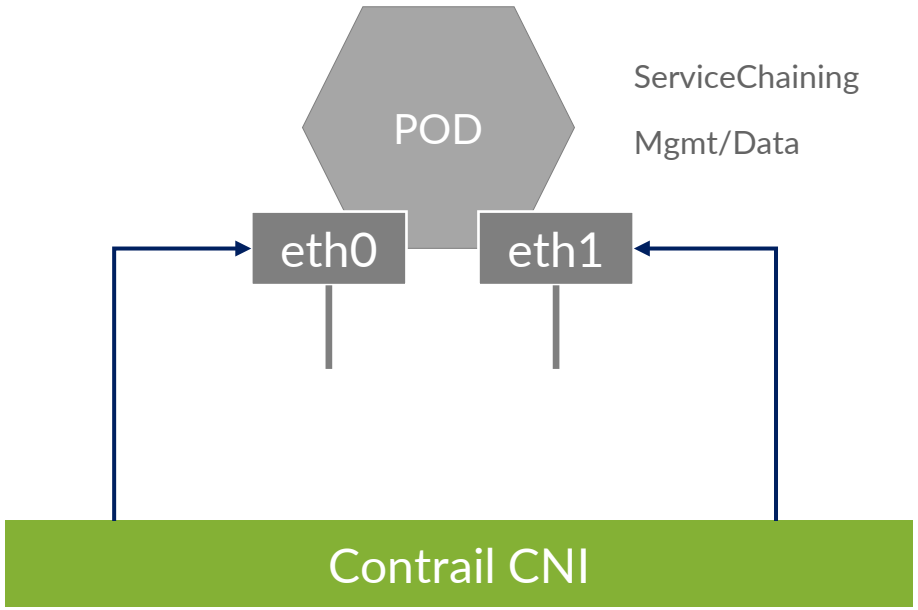




CONTRAIL + KUBERNETES : マルチインターフェース



Multus CNI は、他の CNI プラグインを呼び出すことのできる CNI プラグインです。これにより、他の CNI プラグインを使用して追加のネットワークインターフェースを作成できます。
(引用: REDHAT OpenShift)



Contrail CNIのみで複数のネットワークインタフェースを作成


Thank you
JUNIPER NETWORKS
Driven by Experience™