SDNによるデータセンターのセキュリティー強化

フセイン・カザール

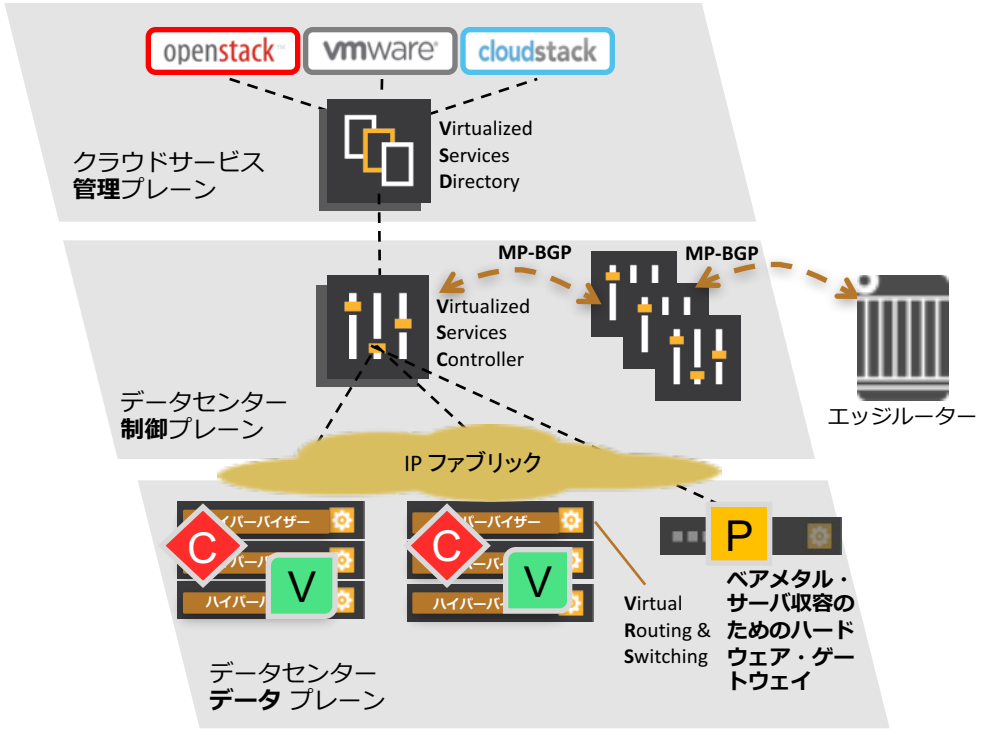
Nuage Networks
ビジネス開発 技術担当上席ディレクター
@hakhazaal

nuagenetworks
From Nokia

Nuage Networks

- シリコンバレーの マウンテン・ビューに本社を設置
- クラウド時代にふさわしいデータセンターネットワークの進化に取り組む、Nokiaのベンチャー企業
- インフラの物理属性、地理的属性を抽象化させ、いかなるワークロードの運用をも支援する、オープン、高性能、スケール性のあるSDNソリューションのご提供
- OpenStackコミュニティー・メンバー

Nuage Networks VSPのアーキテクチャ



Nuage Networks
Virtualized Services Platform (VSP)

Virtualized Services Directory (VSD)
- ネットワークのポリシー・エンジン – 複雑性の抽象化
- サービス・テンプレートと分析

Virtualized Services Controller (VSC)
- SDNコントローラー - ネットワークのプログラム・エンジン
- ALU 7x50 OS を使用した豊富なルーティング機能群

Virtual Routing & Switching (VRS)
- L2-4機能を実装した分散型仮想スイッチ・ルーター
- ベア・メタル資産との統合支援

新しいセキュリティー要件をドライブするマーケット・トレンド

クラウドへの移行

- セキュリティー対応の自動化
- マルチ・テナント対応
- モバイル機器運用のサポート

脅威の拡散への対策

- 脅威の拡散の緩和
- 東西トラフィックの可視化
- 迅速な対応

既存のデータセンターセキュリティーモデルにおける課題

防御

検出

対策

SDNはこのような課題への対応をご支援できます！

既存のアプローチでは不十分

防御

- 境界対策中心 - 全てのアプリとテナント間での信頼が必要
- 内部におけるセグメンテーションの遂行が不能

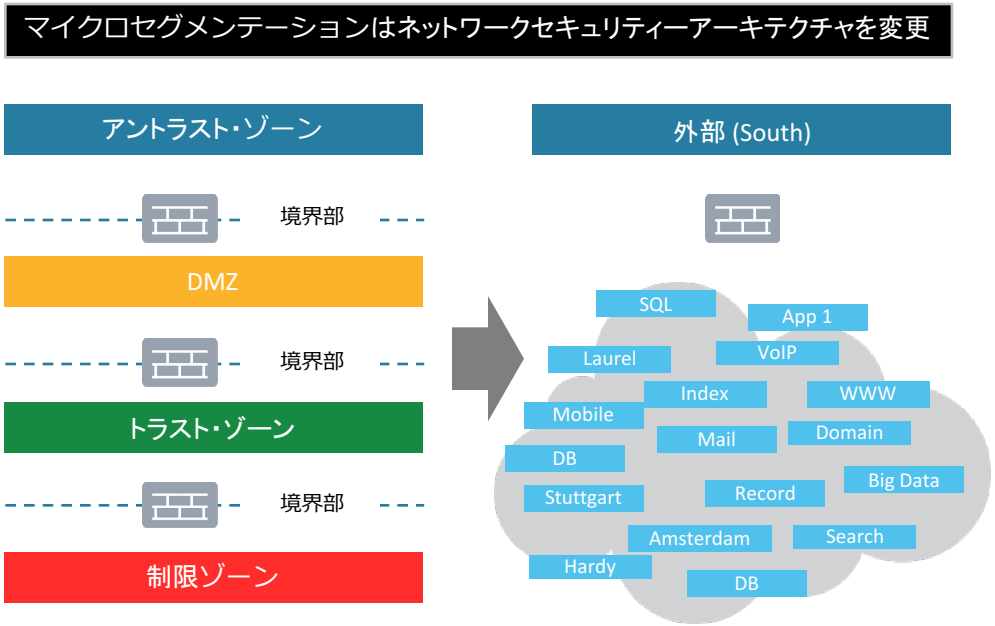
検出

- データセンターの東西トラフィックの可視化や制御が欠如
- 従来のアプローチはクラウド向きのスケール性が提供不能

対策

- 手動対応ではポリシーの更新やアプリのデリバリーが遅延
- 修正対応、管理、更新処理のコストが高い

マイクロセグメンテーションは”ゼロトラスト”モデルでリスクを低減

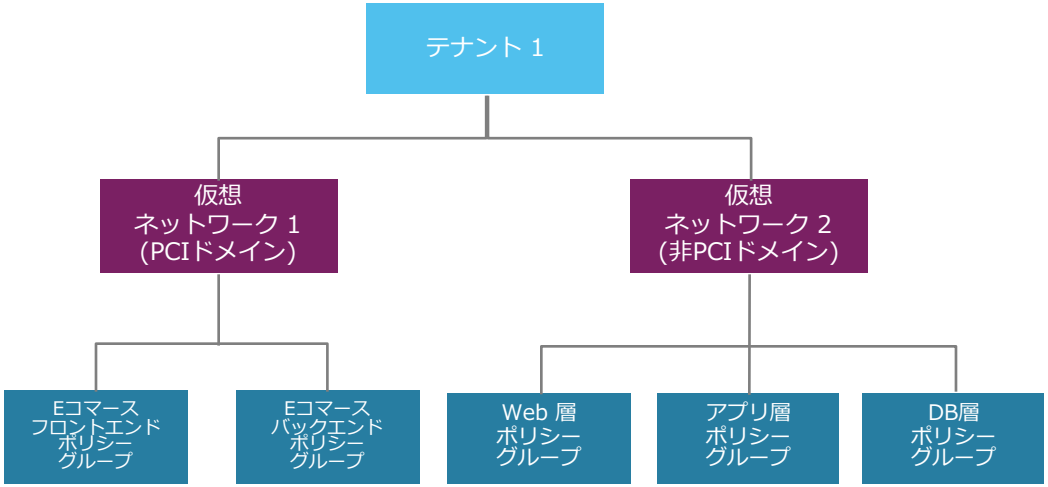


- **利便性**
  - 場所を選ばすエンドポイント間のセキュリティーを保全
  - マルウェアの拡散を規制
- **ユースケース**
  - 高価値資産の保護
  - PCIコンプライアンス環境の実装
  - 共有サービスへのアクセス制限
  - アプリの東西トラフィックの保全

Gartner, Network Security Architectures for Virtualized Data Centers, Joerg Fritsch, 10 August 2015 ; Figure2

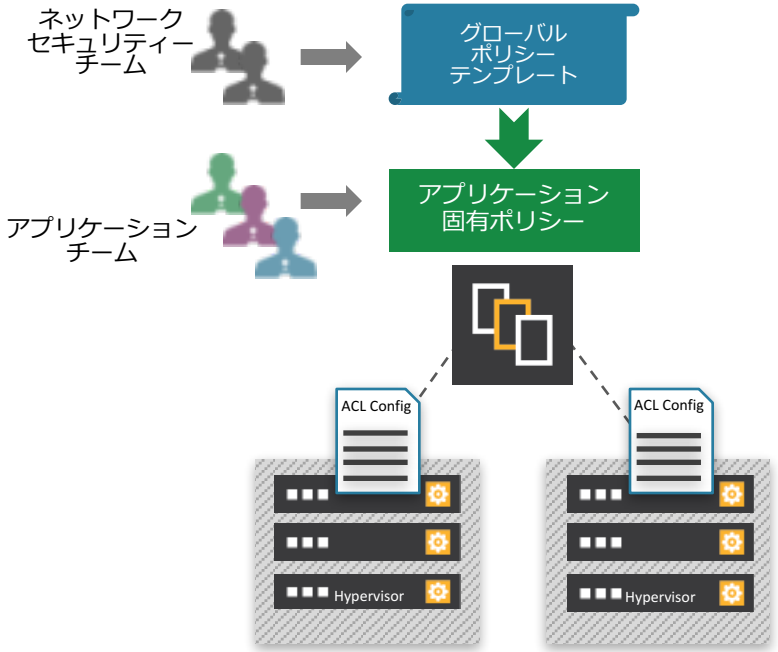
Forrester, Five Steps To A Zero Trust (ZT) Network, John Kindervag, July 27, 2016

Nuage VSPはいかなるエンドポイントに対しても柔軟なセグメンテーションを提供



- マルチテナント運用の保全
- 仮想ネットワークベースの分離機能
- ポリシーグループ設定を利用した論理的なセグメンテーション
- 分散型L4ステートフル・ファイアウォール
- ベアメタル・サーバ、VM、コンテナのサポート

Nuage Networks VSPによるセキュリティー対策の自動化



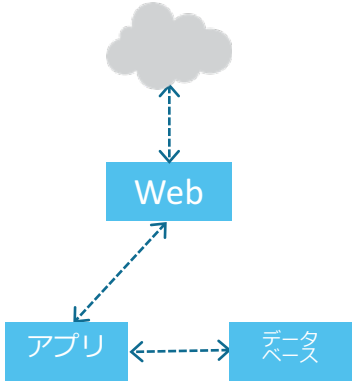
コンプライアンス保全のため, エンタープライズ品質の
広範なセキュリティー設定の**自動化**

ワークロードの生成、削除と同時タイミングでの
セキュリティー設定の**自動化**

転送ポリシーベースでのセキュリティ・サービス定義の
追加・挿入の**自動化**

仮想ネットワークにおける可視化とセキュリティー監視

- ACLフローのロギング
- ポリシーベースのミラーリング

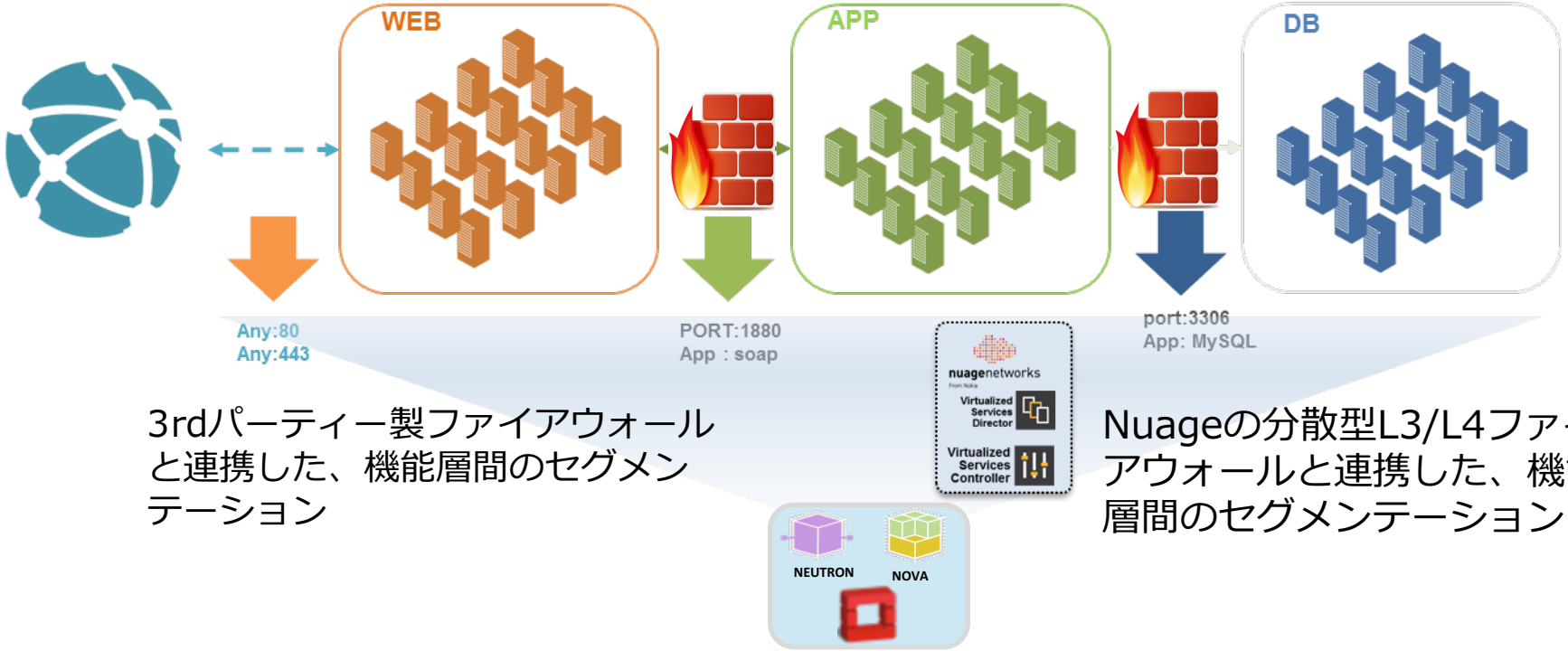


- コンテキスト属性を伴うフローの可視化
- アプリケーションのフローの検出

- セキュリティー警報
- 監視報告

ユースケースの例

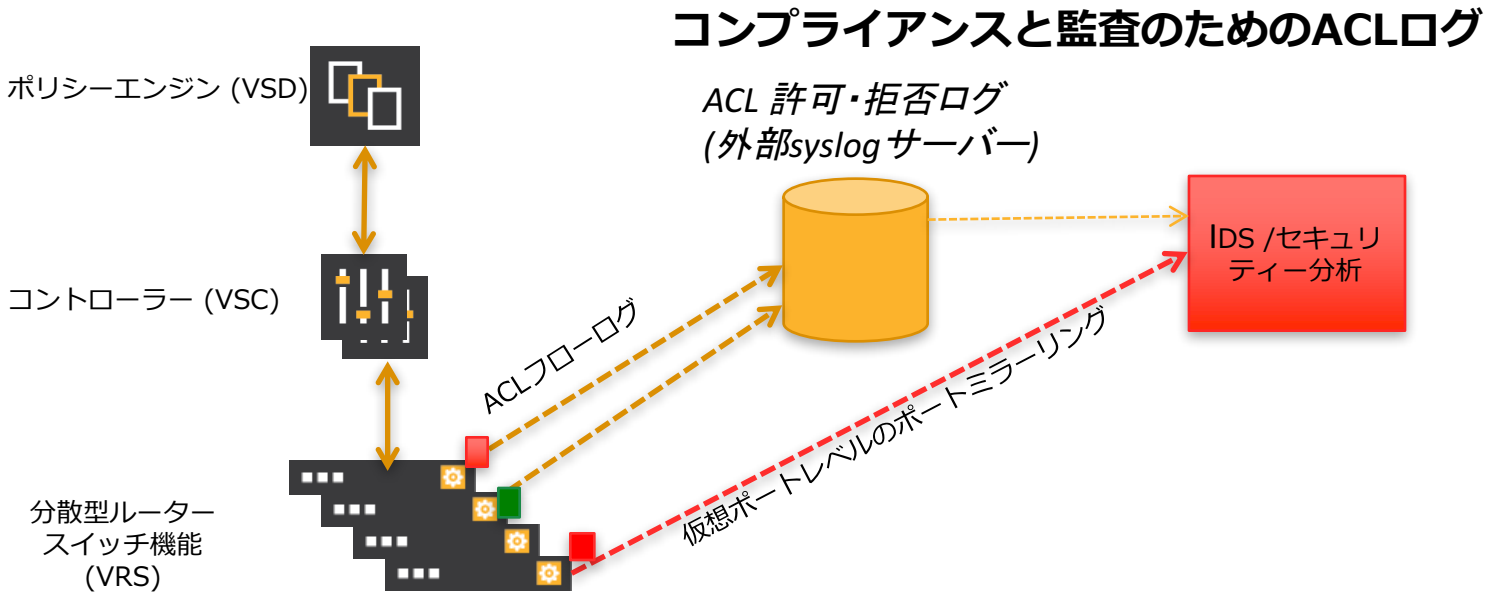
脅威に対する先進的な検出機能をもつ、ネットワークレベルならびにアプリレベルでのマイクロセグメンテーション



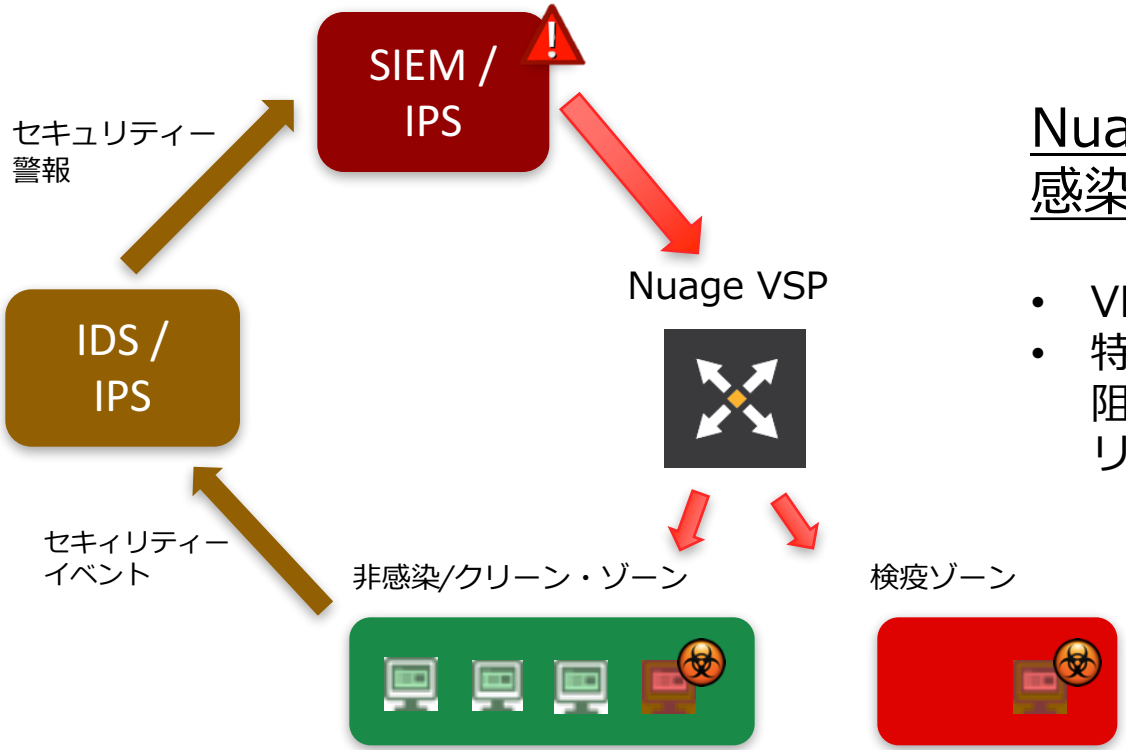
3rdパーティー製ファイアウォールと連携した、機能層間のセグメンテーション

Nuageの分散型L3/L4ファイアウォールと連携した、機能層間のセグメンテーション

より優れた可視化性能、コンプライアンス機能、 脅威の迅速な検出機能



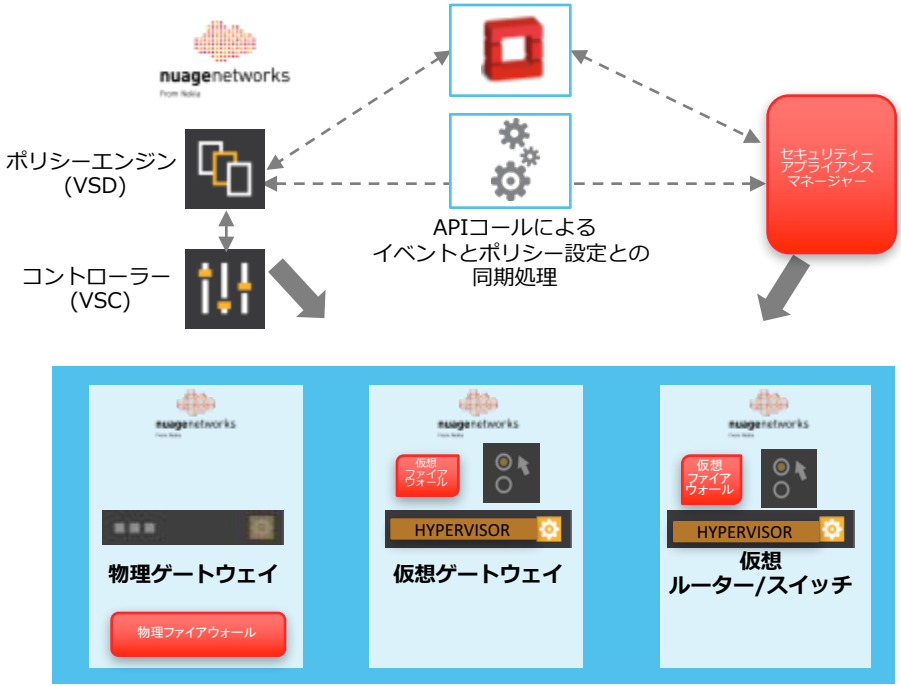
迅速な有事対応　[自動検疫]



Nuage VSP APIを運用し、感染サーバやVMを検疫

- VMを検疫ゾーンに移動
- 特定の通信(例、C&C, FTP)を阻止すべくセキュリティーポリシーを適用

Nuage Networks VSPと業界の主導的な製品との統合

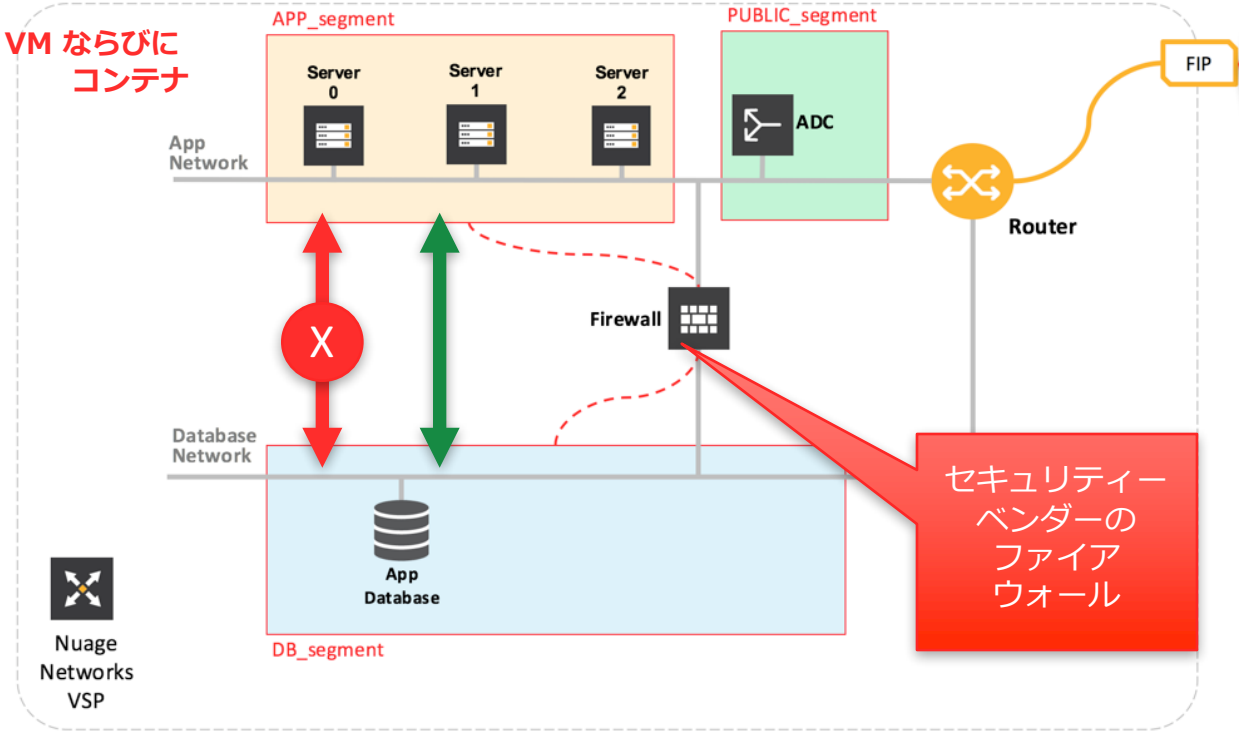


- **セキュリティー設定の自動化**
  - ポリシーベースによる、物理実装または仮想実装のセキュリティーサービスの挿入
  - ワークロードの種類を選ばない、ポリシーベースのセキュリティー設定の自動化
- **先進のセキュリティー制御**
  - アプリケーションベースのマイクロセグメンテーション
  - 脅威の先進的な検出機能の実装

パートナー製品との統合による先進的なセキュリティーソリューション

- 広範なエコシステム連携による保護
- データセンター内での先進的なマイクロセグメンテーション、脅威の検出、自動検疫を可能にするソリューション
- 物理、仮想のアプライアンスを用いる、柔軟なセキュリティーサービスの追加挿入
- 既存のセキュリティー・アプライアンスや運用モデルと共存しうる、投資保護

デモ



Nuage Networks VSPによる、クラウドとエンタープライズデータセンターにおけるセキュティー課題への対応

プライベート・クラウド、パブリック・クラウドのためのマルチテナント環境の保全	✓ リスクの低減、並びに、インフラコストの低減 ✓ クラウドサービスプロバイダーによる、ネットワークセキュリティーのサービス化の提案を実現
マイクロセグメンテーションによるマルウェアの拡散防止	✓ 先進的なL4-7セキュリティサービスの挿入と、分散型組み込みL4ファイアウォールとの連携運用 ✓ 物理、仮想、コンテナなど、多様なワークロード、マルチハイパーバイザー、多様なネットワークの保護
ポリシーベースのセキュリティー設定の自動化とコンプライアンスの実現	✓ 論理的なコンテキストとグルーピングとに基づくポリシー運用 ✓ L4セキュリティーとコンプライアンスとを実現させる、自動的なプロビジョニング機能
自動検疫による迅速な有事対応	✓ APIを使用し、脅威検出/SIEMシステムとの統合による、自動検疫

ご清聴ありがとうございました!

詳細な製品情報をお求めの方は、是非ともOpenStack Days Tokyo 2016の弊社のブースか、次のWebサイトにお立ち寄りください。
www.nuagenetworks.net/partners

ご質問の方は, 次のあて先までご連絡ください。
jpn@nuagenetworks.net
partners@nuagenetworks.net

nuagenetworks