vFORUM

NS153

ついに来た！ マイクロセグメンテーションの 物理サーバ対応を徹底解説！

ヴイエムウェア株式会社
ソリューションビジネス本部
システムズエンジニア　金巻 賢二郎

#vforumjp

vmware

免責事項

- このセッションには、現在開発中の製品/サービスの機能が含まれている場合があります。
- 新しいテクノロジーに関するこのセッションおよび概要は、VMware が市販の製品/サービスにこれらの機能を搭載することを約束するものではありません。
- 機能は変更される場合があるため、いかなる種類の契約書、受注書、または販売契約書に記述してはなりません。
- 技術的な問題および市場の需要により、最終的に出荷される製品/サービスでは機能が変わる場合があります。
- ここで検討されているまたは提示されている新しいテクノロジーまたは機能の価格およびパッケージは、決定されたものではありません。

Agenda

Virtual Cloud Network

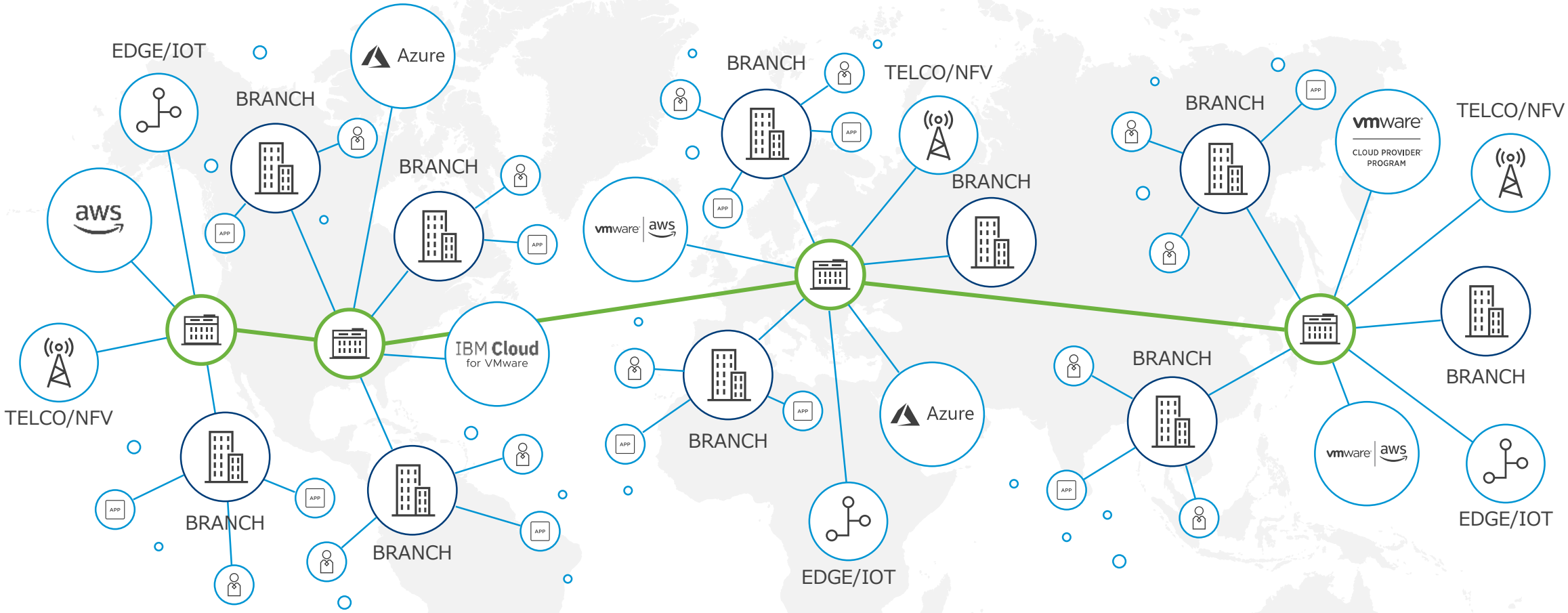
物理サーバへのマイクロセグメンテーション
4つの適用方法

VMware NSX® Data Center の アリスタ クラウドビジョン連携

アリスタクラウドビジョン連携デモ

The Virtual Cloud Network

Click to edit optional subtitle

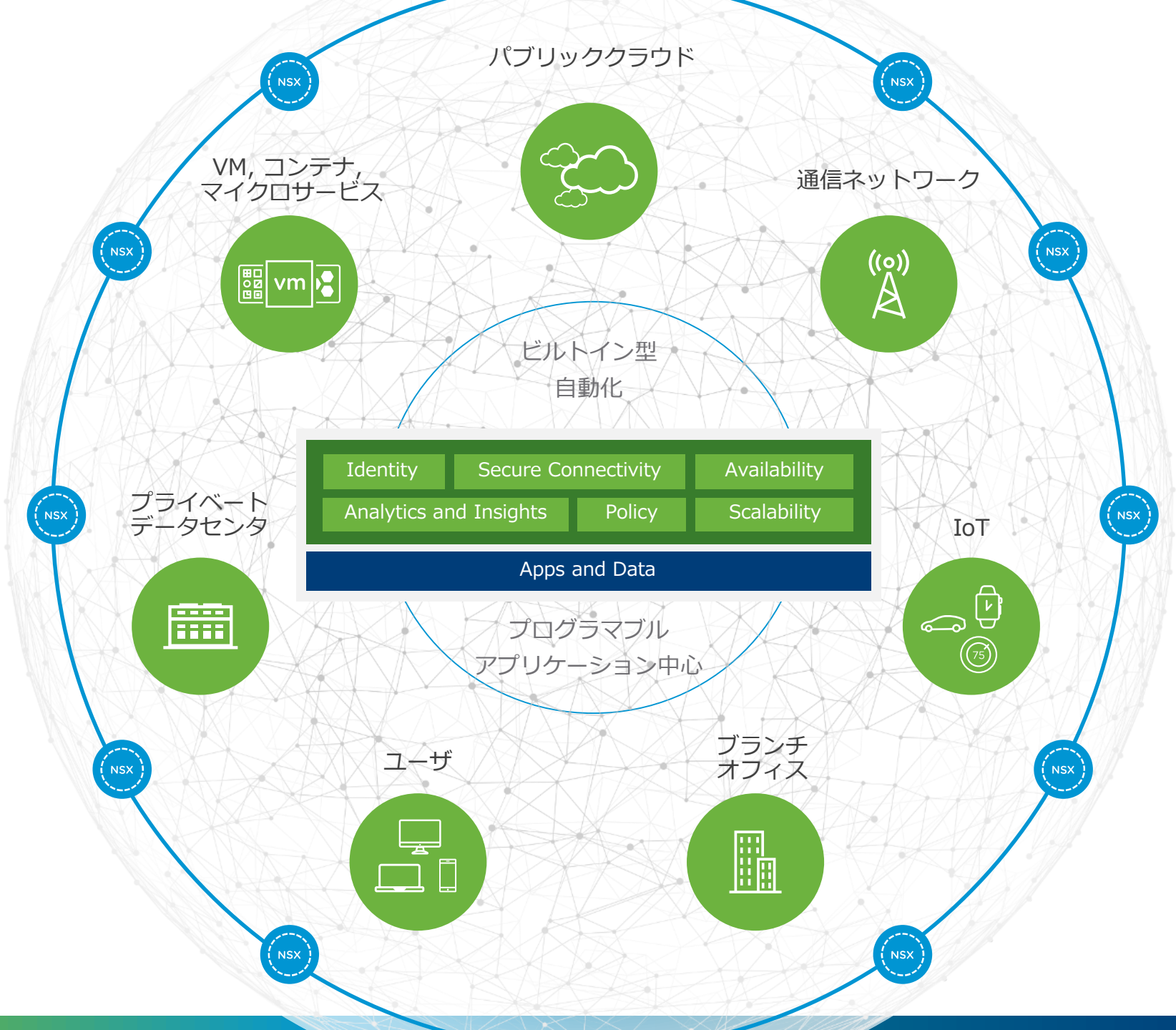


The Virtual Cloud Network

ビジネスを守り、つなぐ

Virtual Cloud Networking

Connect & Protect
any workload across
any environment



様々なサーバコンピュータ

新たなネットワークとセキュリティ要件

VM の急増と
ネットワーク仮想化

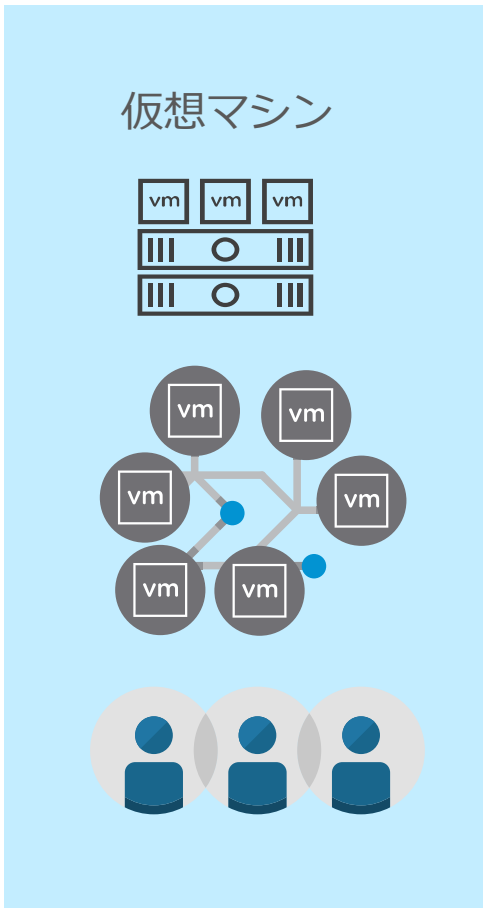
コンテナネットワークへの
マルチテナント、マイクロ
セグメンテーション、およ
び運用管理ツール

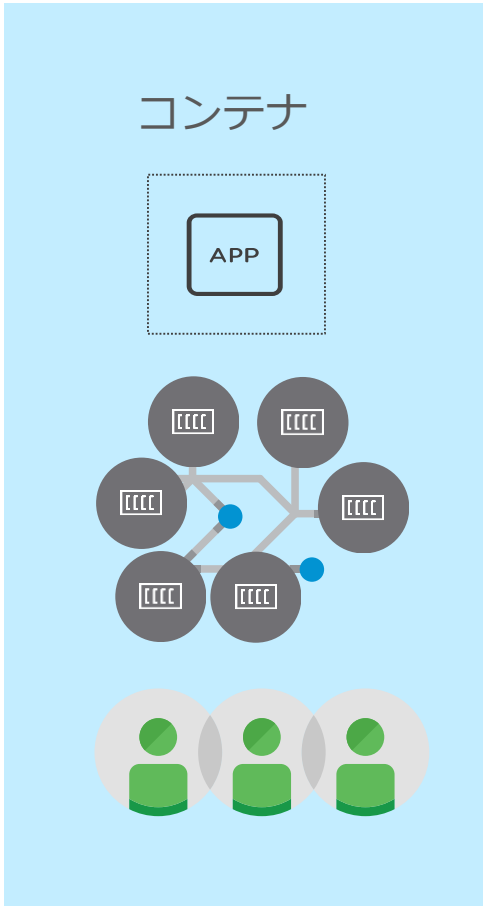
プライベートクラウドとパブ
リッククラウド間で一貫性の
ある操作で完全な可視性と
制御

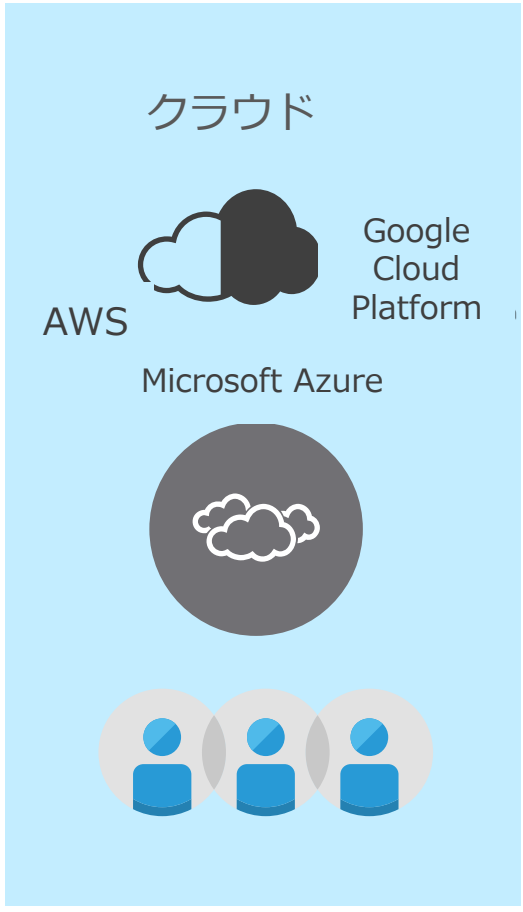
物理ワークロード（レガシー
アプリケーション、DB、スト
レージ、セキュリティアプラ
イアンス）のシームレスな
接続性とセキュリティ

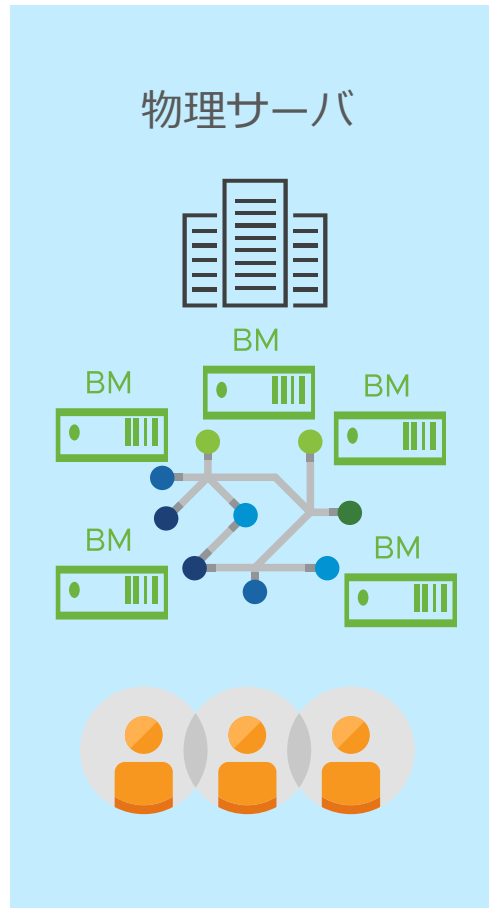
新たなサイロ化が業務の非効率性を生む

課題：技術スタック、プロセス、チーム、専門技術の違い

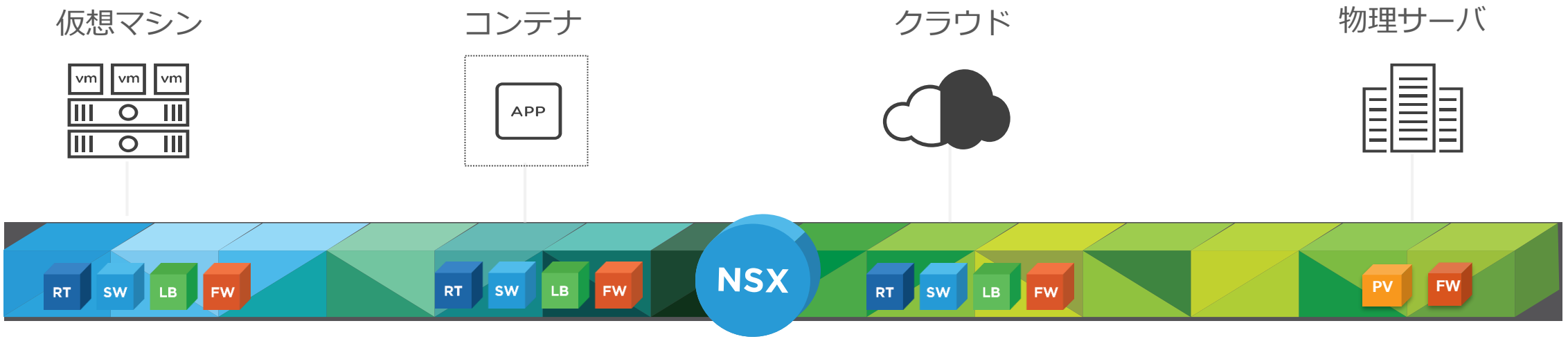








NSX：すべてのワークロードのためのプラットフォーム



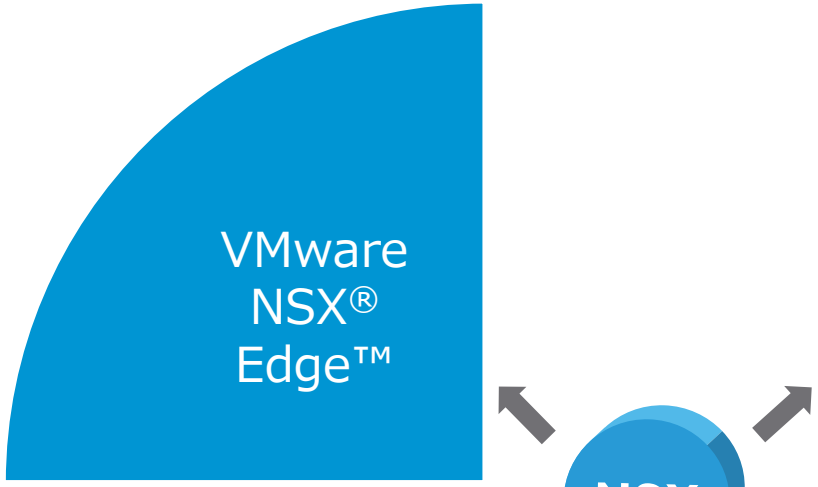
- プライベートクラウドとパブリッククラウドの統一されたネットワーキングとセキュリティサービス
- 統合された管理
- インフラをサポート

物理サーバへの
マイクロセグメンテーション

単一の管理プラットフォームによる
セキュリティ施行

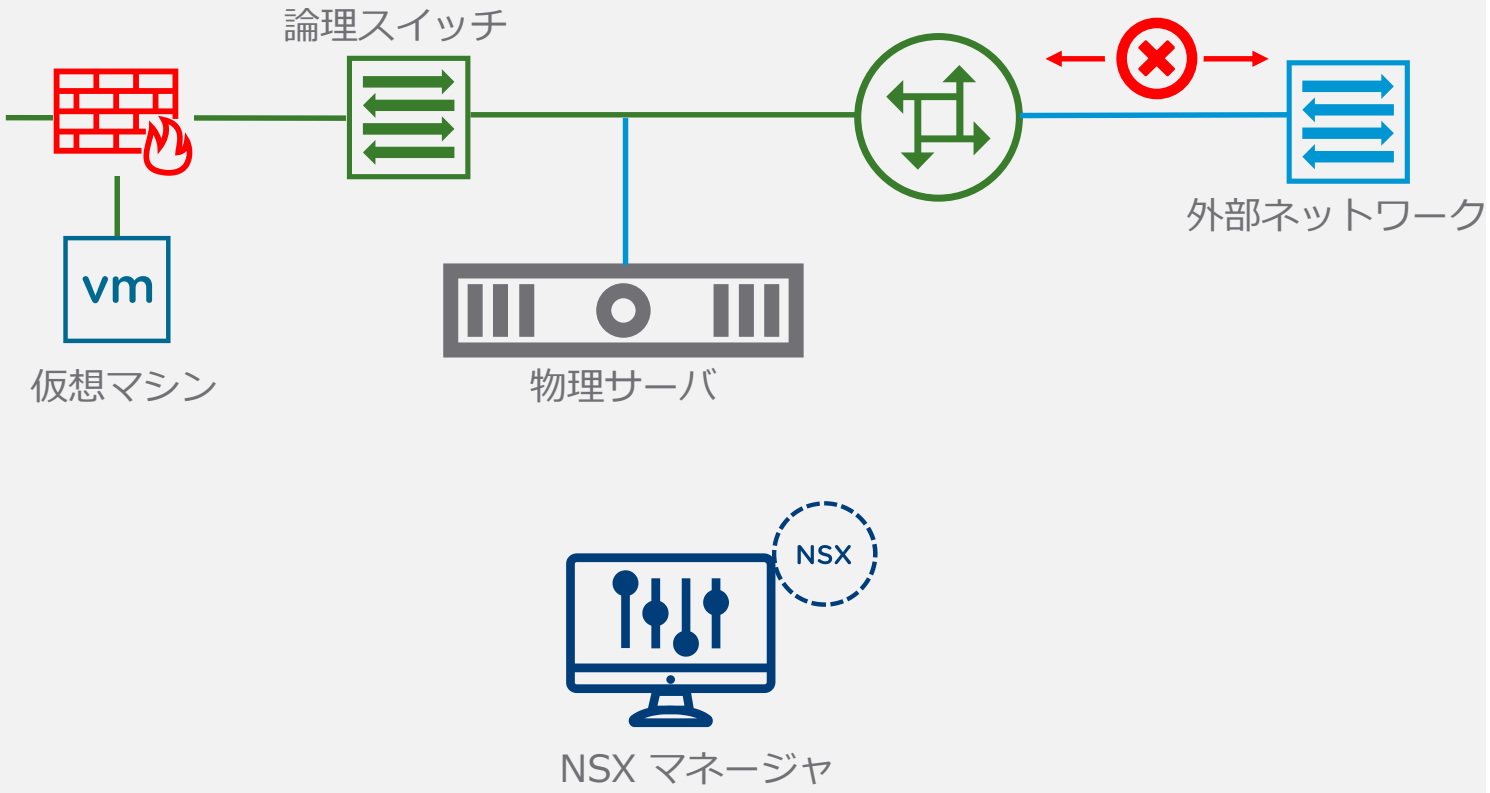
4つのセキュリティ適用方法

シングル管理プラットフォームとしての NSX



NSX エッジでの仮想および物理的なセグメント化

シングル管理プラットフォームとしての NSX

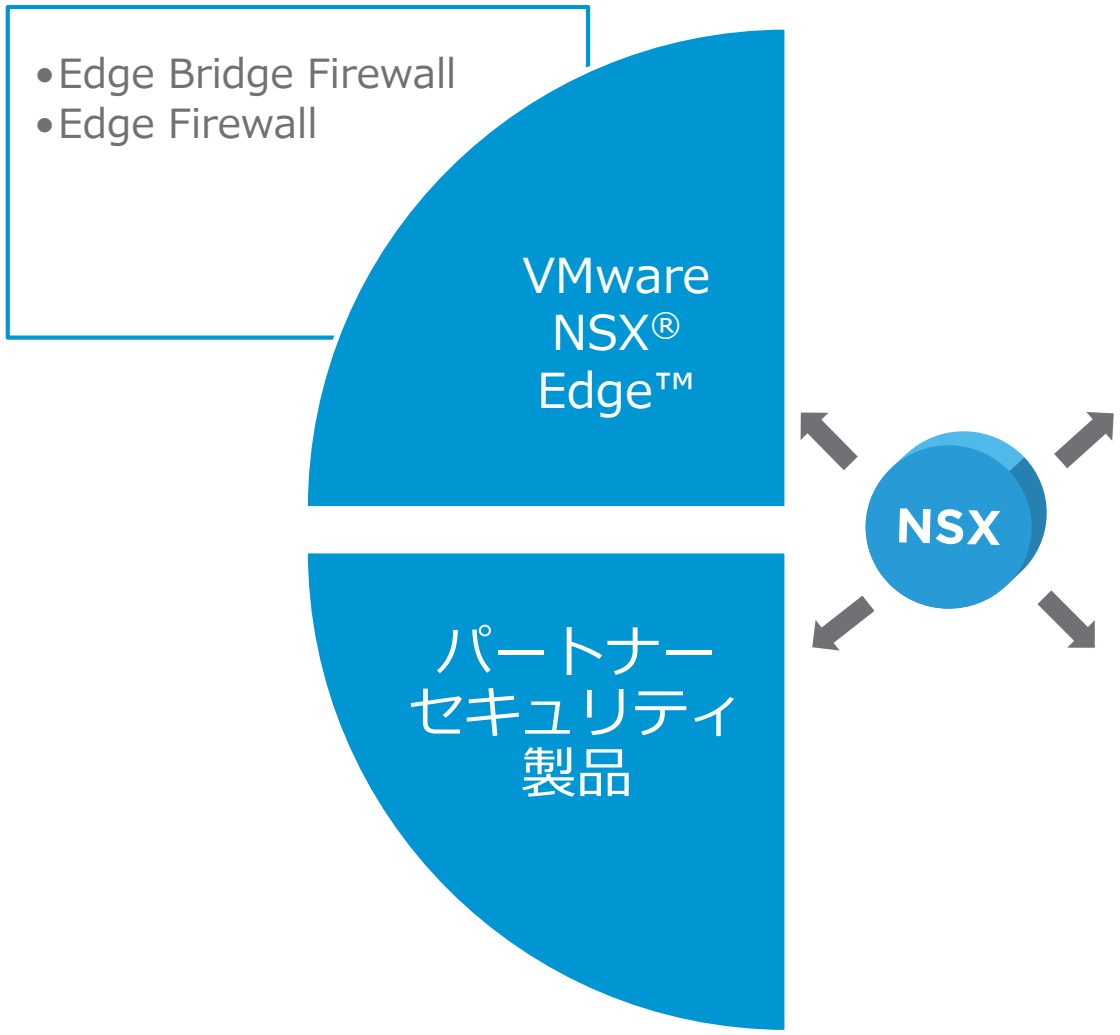


物理サーバへの南北トラフィック

エッジファイアウォールで
外部からの通信をステートフル
L4 ファイアウォールを適用

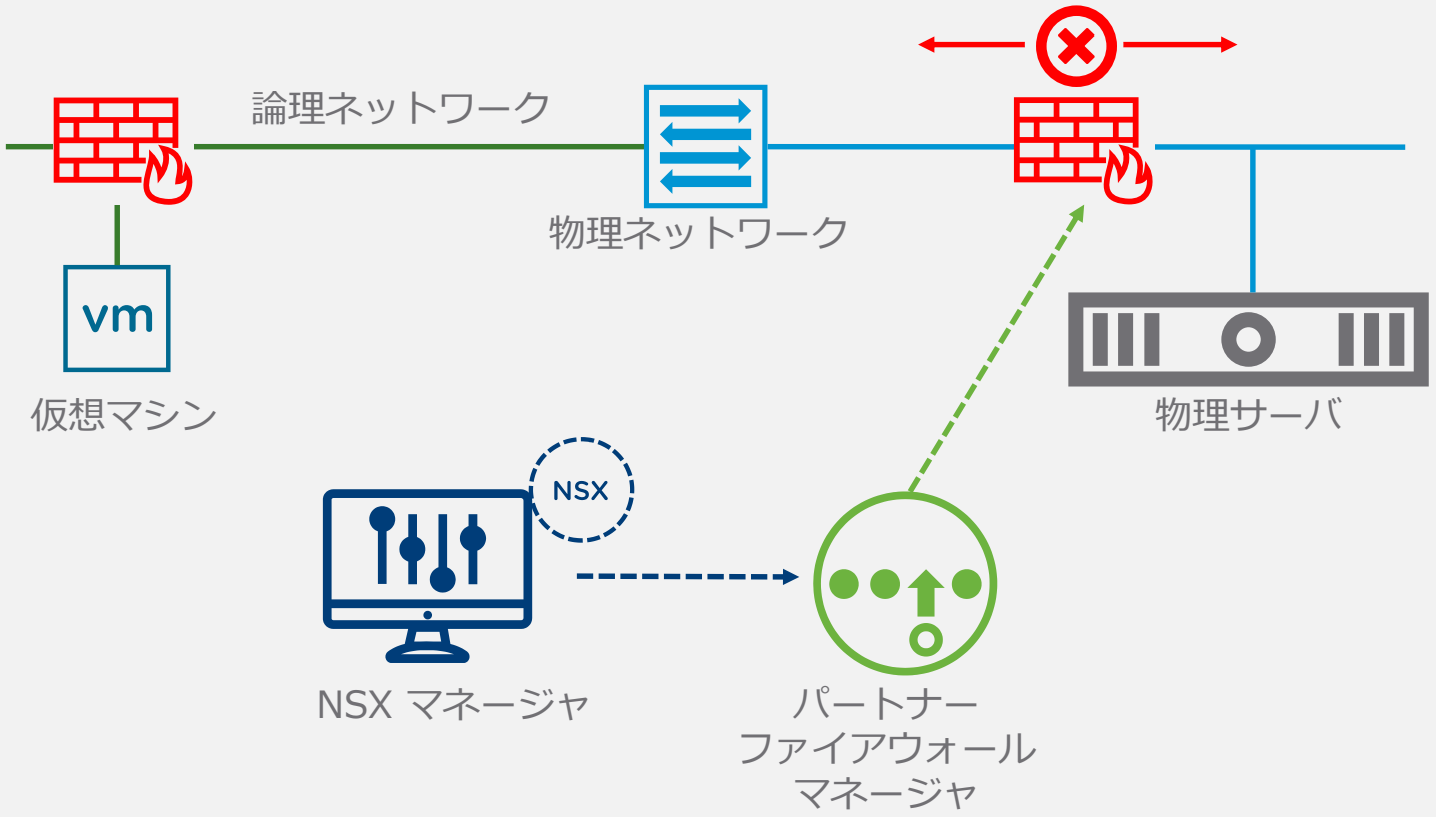
4つのセキュリティ適用方法

シングル管理プラットフォームとしての NSX



パートナーファイアウォールによるセグメント化

シングル管理プラットフォームとしての NSX

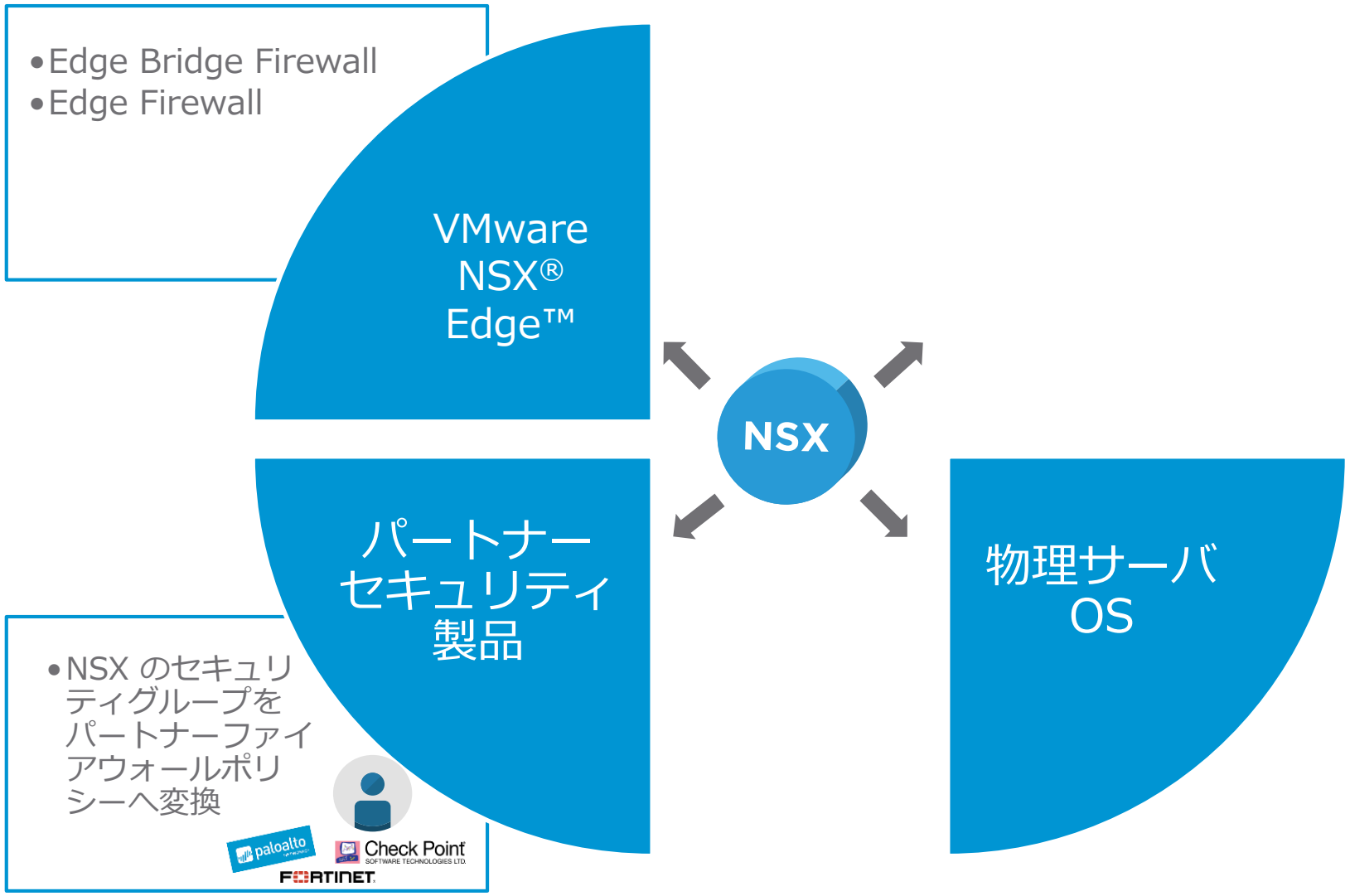


パートナーファイアウォールソリューションとの NSX の統合により、仮想から物理への通信を規制することが可能

NSX のセキュリティグループをパートナーファイアウォールマネージャと交換し、実際のポリシーへ変換

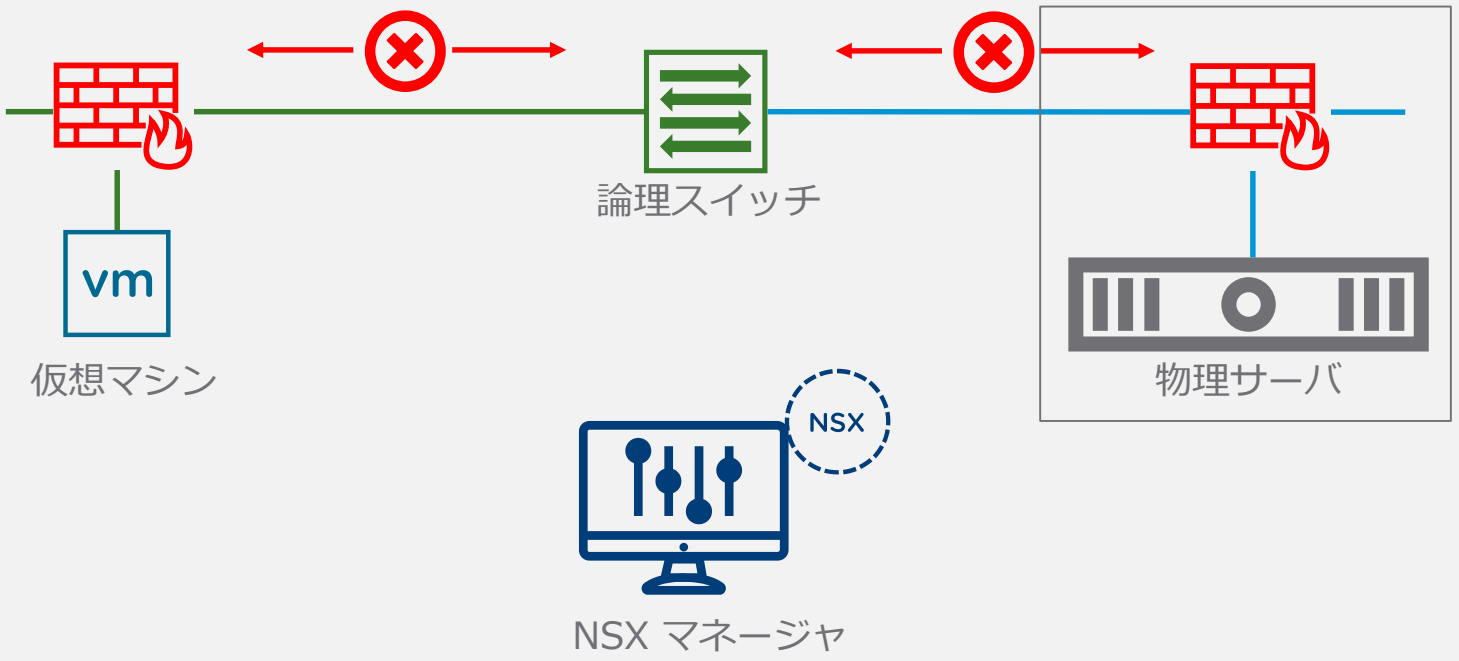
4つのセキュリティ適用方法

シングル管理プラットフォームとしての NSX



物理サーバ内部でのマイクロセグメンテーション

シングル管理プラットフォームとしての NSX

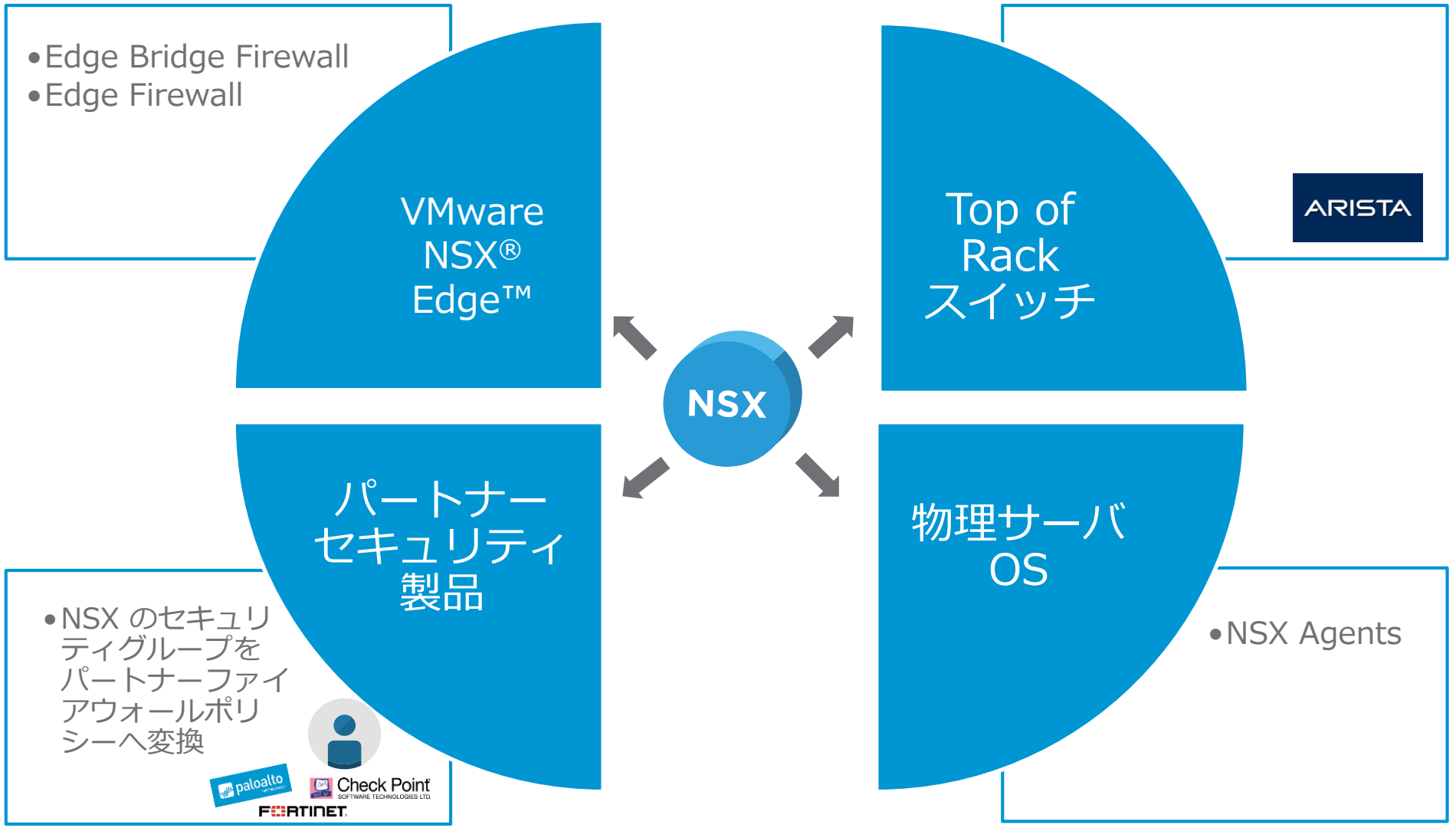


物理サーバにて入出力トラフィックをフィルタ

物理サーバの OS に OVS ベースの NSX エージェントをインストール

4つのセキュリティ適用方法

シングル管理プラットフォームとしての NSX



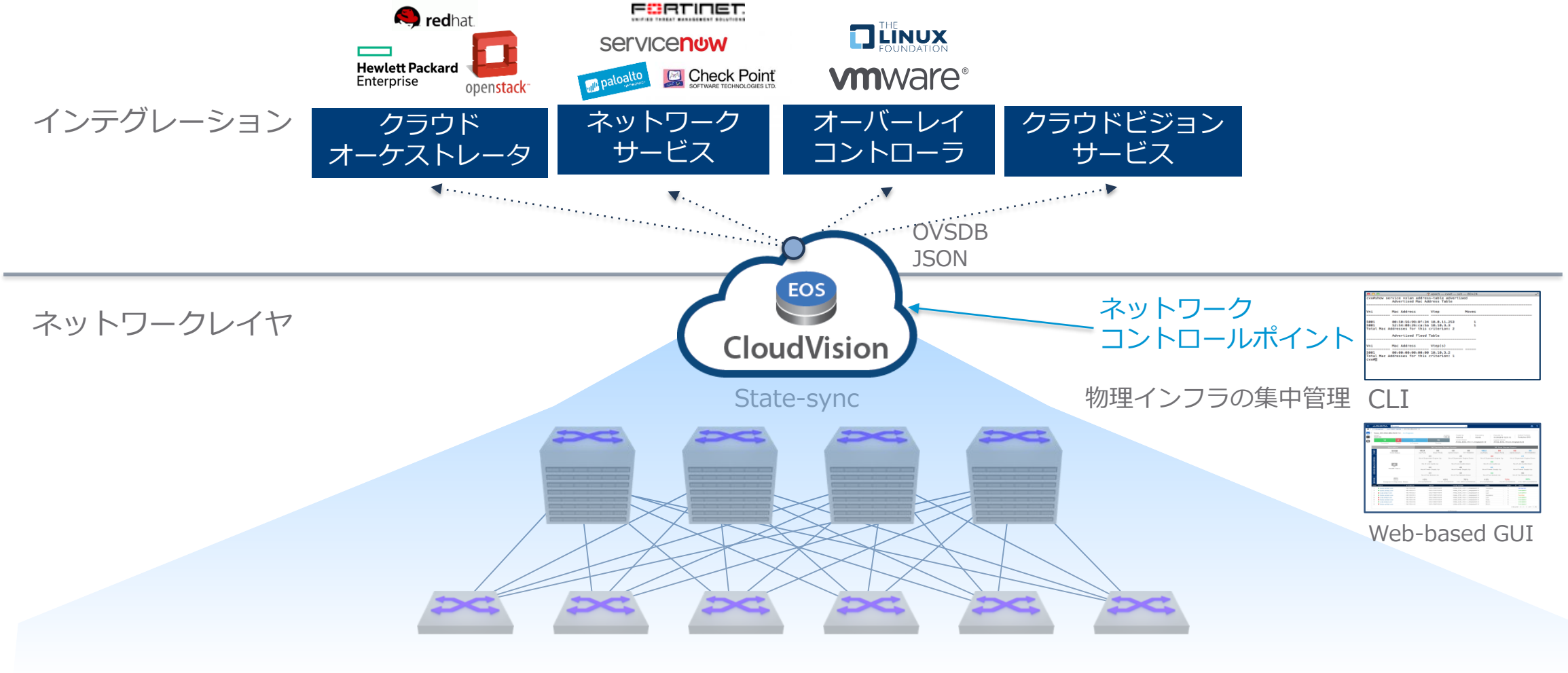
VMware NSX Data Center のアリスタ クラウドビジョン連携

コンセプト

注：このソリューション現在開発中となります

アリスタ クラウドビジョン

アンダーレイへの統合ポイント

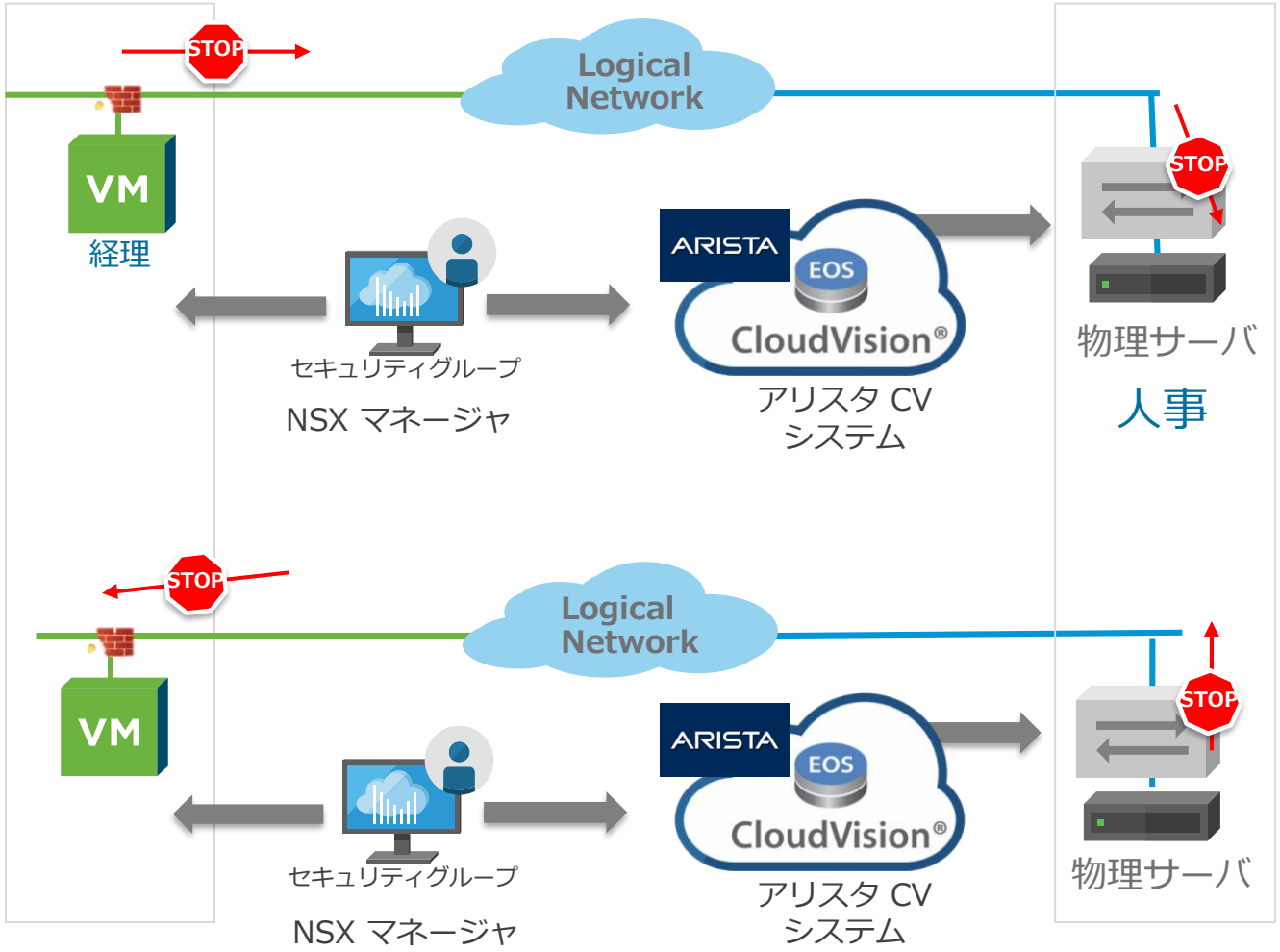


ネットワーク全体の自動化と可視化のためのプラットフォーム

ユースケース 1

アリスタクラウドビジョンによる ToR マイクロセグメンテーション

仮想 – 物理間通信のためのマイクロセグメンテーション



- 物理サーバへの入出力トラフィックをフィルター（サブネット間/内問わず）

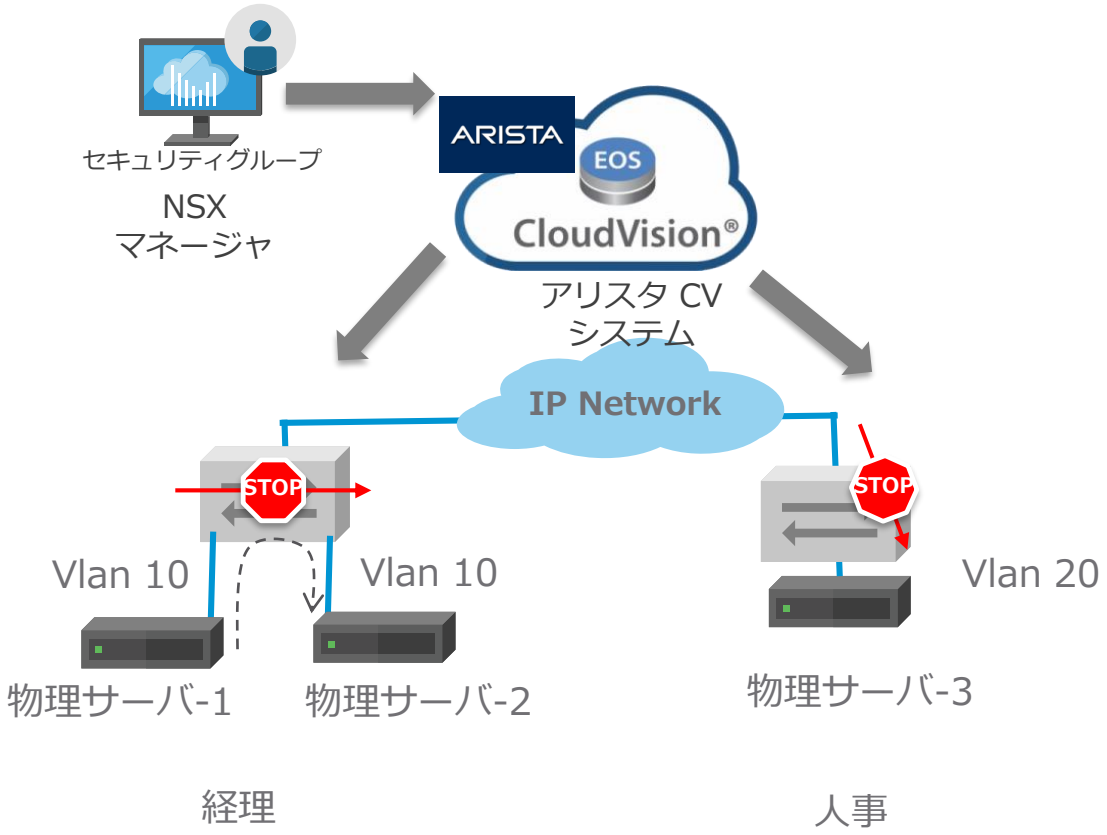
アクセスコントロールリストを
ToR スイッチへプログラム

注：このソリューション現在開発中となります

ユースケース 2

アリスタクラウドビジョンによる ToR マイクロセグメンテーション

物理 – 物理間通信のためのマイクロセグメンテーション



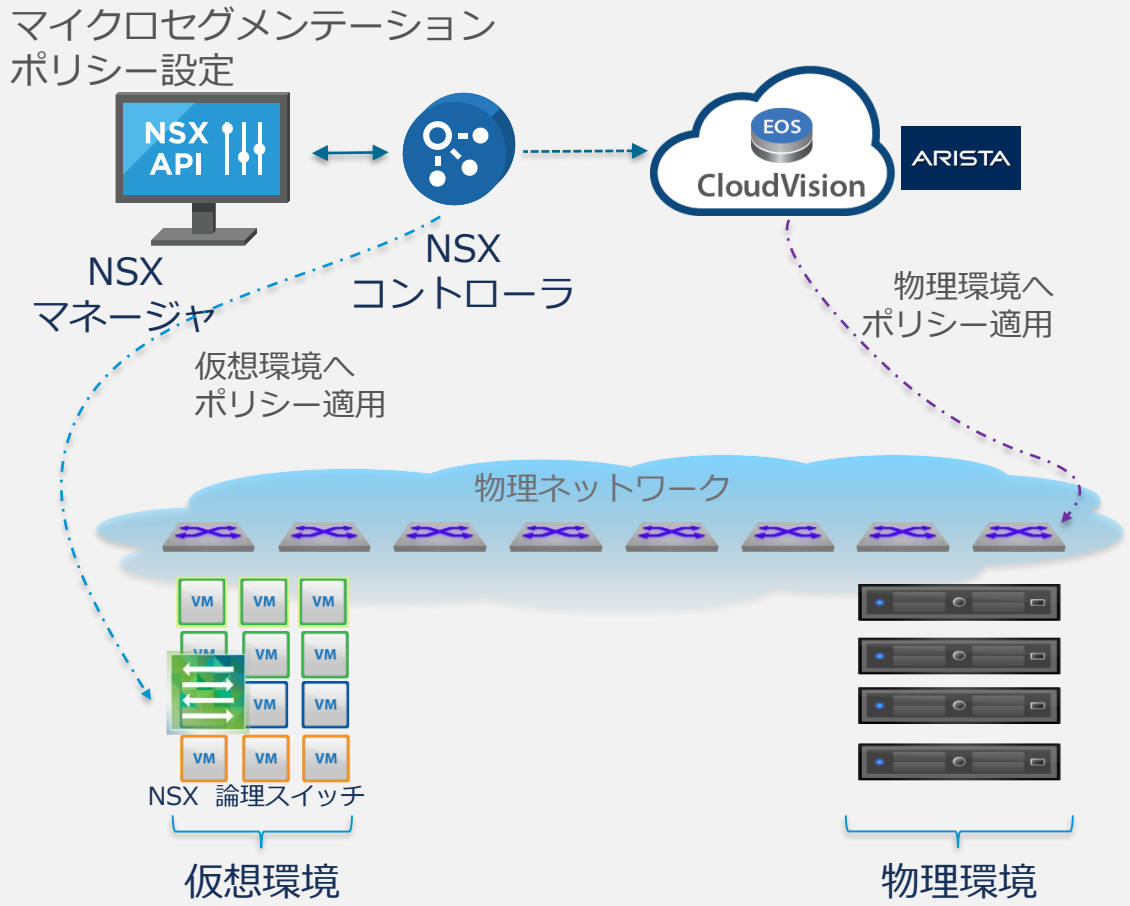
- 物理サーバ間のトラフィックをフィルター (サブネット間/内問わず)

アクセスコントロールリストを
ToR スイッチへプログラム

注：このソリューション現在開発中となります

アーキテクチャ

アリスタクラウドビジョン連携



機能

仮想と物理サーバへ共通のポリシーを適用

ToR スイッチへはアリスタクラウドビジョンを通して動的に ACL を適用

メリット

NSX が仮想だけではなく物理サーバ環境への単一のセキュリティ制御ポイントとなる

アリスタ Leaf スイッチ への ダイナミックなポリシー適用

物理および仮想環境に対して一貫したセキュリティと管理環境を提供

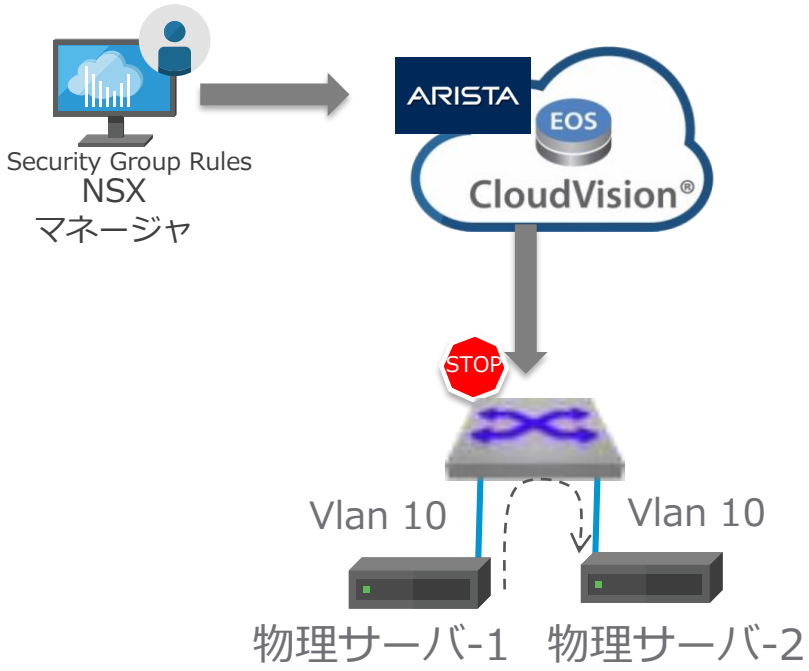
注：このソリューション現在開発中となります

アリスタクラウドビジョン
連携デモ

注：このソリューション現在開発中となります

デモ構成

物理サーバ間通信へのマイクロセグメンテーション

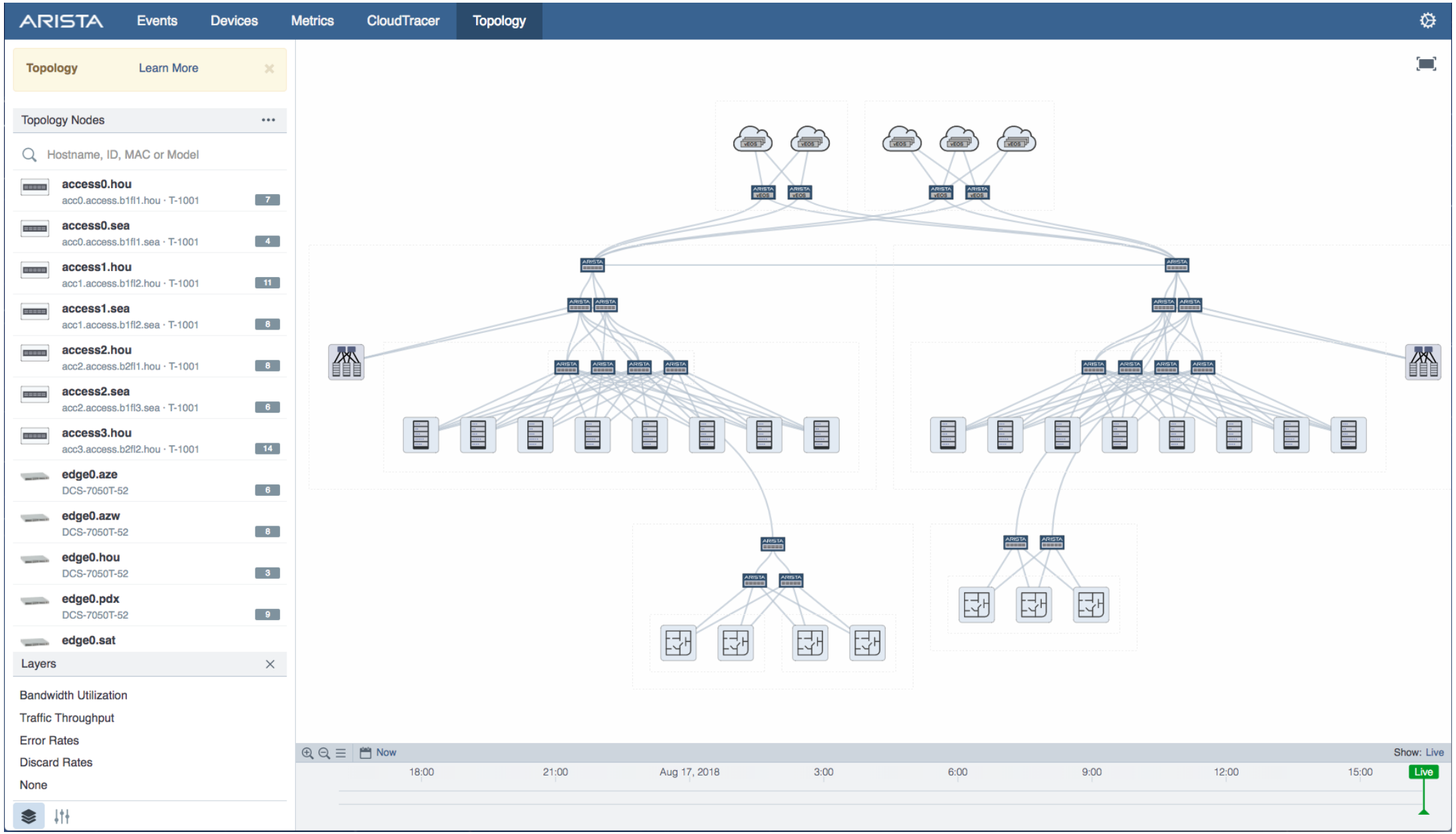


デモ手順

1. ポリシーがない状態で物理サーバ間の通信が通ることを確認
2. NSX マネージャと連携したクラウドビジョンからフィルターポリシーの設定
3. リアルタイムにポリシーが書き換えられることろ確認

注：このソリューション現在開発中となります

アリスタ クラウドビジョン UI



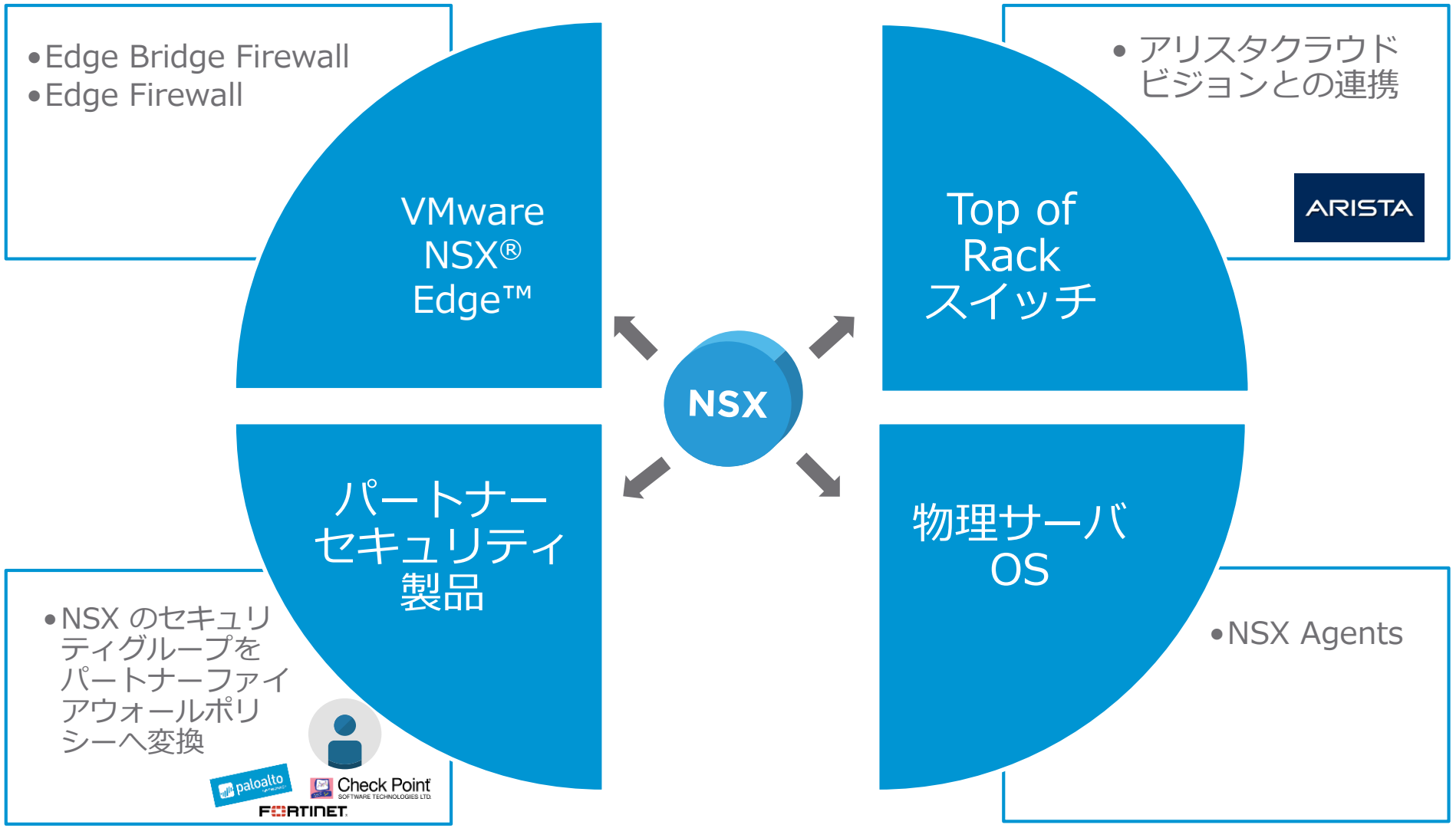
shadabs — a7050# — ssh 10.33.86.75 -l admin — 181×48

~ — a7050# — ssh 10.33.86.75 -l admin | ~ — cvx# — ssh 10.172.121.119 -l admin | root@dfw-vmw-demo-2: ~ — ssh 10.33.87.232 -l... | vmware@dfw-vmw-demo: ~ — ssh 10.33.86.220...

```
a7050#
```

4つのセキュリティ適用方法

シングル管理プラットフォームとしての NSX



ご清聴、ありがとうございました。