【トレノケート 共催】

Cisco Support Community Expert Series Webcast

Cisco ACI 入門

日鷹 仁司 (Hitoshi Hidaka)
トレノケート 株式会社
Cisco 認定インストラクター

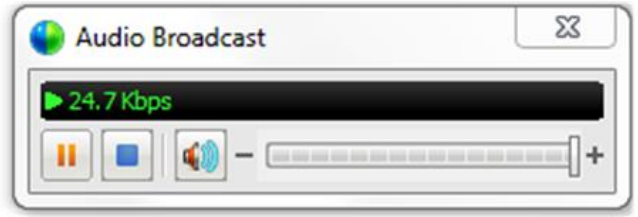
2018/6/26

ご参加ありがとうございます。

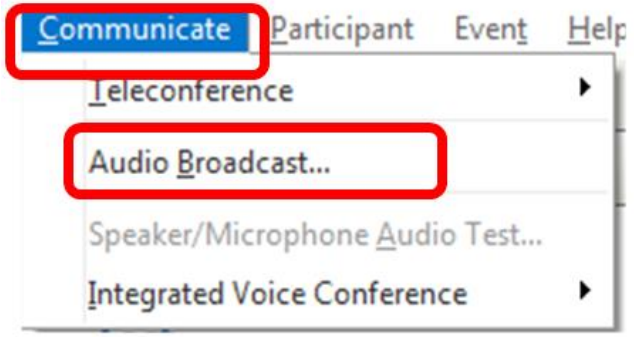
本日の資料はこちらからダウンロードいただけます。
https://supportforums.cisco.com/t5/-/-/ba-p/3392410

オーディオ ブロードキャスト について

[Audio Broadcast （オーディオ ブロードキャスト）]
ウィンドウが自動的に表示され、コンピュータの
スピーカーから音声が流れます。



[Audio Broadcast （オーディオ ブロードキャスト）]
ウィンドウが表示されない場合は、[Communicate
（コミュニケート）] メニューから [Audio Broadcast
（オーディオ ブロードキャスト)] を選択します。



イベントが開始されると自動的に音声が流れ始めます。

音声接続に関する詳細はこちらをご参照ください。
解決しない場合は、 QA ウィンドウよりお知らせください。
https://supportforums.cisco.com/ja/document/82876

ご質問方法

Webcast 中のご質問は全て画面右側の QA ウィンドウより
All Panelist 宛に送信してください。

エキスパート スピーカー

日鷹 仁司 (Hitoshi Hidaka)

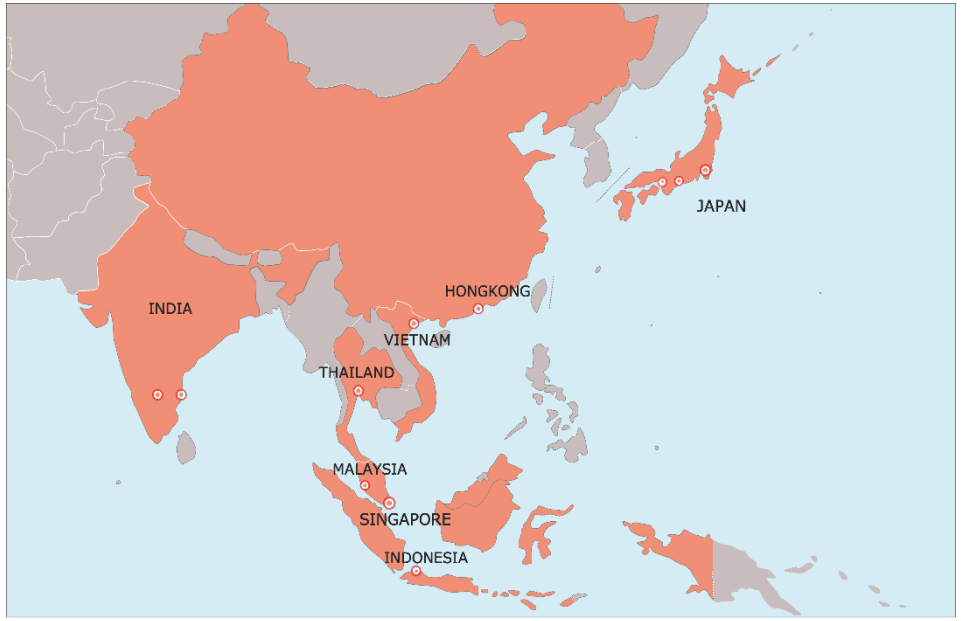
トレノケート 株式会社

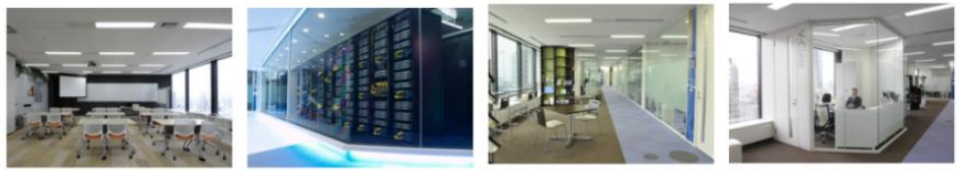
Cisco 認定インストラクター

トレノケート 株式会社

会社紹介とご案内

会社概要





東京 21教室/大阪 4教室/名古屋3教室/
オンライン配信スタジオ完備

■名称　：**トレノケート株式会社**
（旧：グローバルナレッジネットワーク株式会社）

■所在地：東京都新宿区西新宿6丁目8番1号
住友不動産新宿オークタワー19～20階

■代表者：小澤　隆

■特徴

ITとビジネストレーニングのリーディングカンパニー

- 日本/シンガポール/インド/インドネシア/マレーシア/タイ/ベトナムなどのアジア諸国で、トレノケートグループとしてグローバルIT人材育成を展開
- 子会社クインテグラル株式会社（旧グローバルナレッジマネジメントセンター株式会社）を通じ、世界最大の人材育成組織 American Management Association のサービスを国内で唯一、提供

AMA American Management Association®

■サービス

- 定期開催コース、一社向け研修、Virtual Classroom、eラーニング、テストセンター、オンライン配信などの多様な研修サービス
- 提供コース数1,000以上、年間定期開催コース数6,000以上
- 一社向け研修では、お客様の課題に合わせた研修の企画から、教材作成、トレーニング実施、終了後フォローまで、柔軟に対応

TRAINOCATE

新ブランド "TRAINOCATE" への変更について

- Global knowledge Asia Pte. Ltd. はアジアでのブランド名を**TRAINOCATE（トレノケート）** へ変更

※ 日本は2017年10月にトレノケート株式会社に社名変更

※ グローバルナレッジネットワーク株式会社時代とサービスに変更はありません

ブランド名の由来

TRAINing

＋

AdvOCATE

人材育成のコアである "Training" と、先導者、提唱者を意味する "Advocate" を合わせた造語です。「トレーニング」分野の「先導者」として、一層の飛躍を目指して名付けました。

ロゴに込めた想い

TRAINOCATE（トレノケート）のロゴは、エベレストをイメージしています。
アジアに位置しながら、世界で最高峰を誇る山を旗印にすることで、
「アジアから世界の頂を目指す」という志を込めています。

TRAINOCATE

トレノケートの Cisco トレーニングの特徴

■ 日本で唯一のシスコ認定プラチナラーニングパートナー

- シスコ認定プラチナラーニングパートナーは世界で17社あり、カスタマイズトレーニングの作成・提供することが出来るラーニングパートナーです。**トレノケートは日本で唯一のプラチナラーニングパートナー**です。

■ Learning Partner of the Year APJ 2018を受賞

- この賞はシスコのトレーニングに対して貢献度が高く、模範的なシスコ認定ラーニングパートナーを表彰するものです。

■ 3名がCisco Instructor Excellence Award を3年連続で受賞

- トレノケート株式会社のシスコ認定インストラクターが、CCIE Routing & Switching 部門において、Instructor Excellence Awardを受賞いたしました。**今回受賞した3名は、2016年から継続して3年連続での受賞となりました。**
- Instructor Excellence Awardとは、テクノロジーごとに各地域（アメリカ、ヨーロッパ、アジア）において最も優れたシスコ認定インストラクターに贈られる賞です。2018年は、日本では４名が受賞し、うち３名がトレノケートのトレーナーです。
- 受賞CCSI氏名：日鷹　仁司、斉藤　理恵、岡本　千賀

TRAINOCATE

トレノケートの Cisco 認定トレーニング

■認定資格対応コースからカスタマイズしたプロダクト（製品）トレーニングまで
幅広いラインナップ

▼コース一覧はこちら▼

https://www.trainocate.co.jp/reference/cisco/ciscolist/course.html

TRAINOCATE

トレノケートの Cisco Data Center コース一覧

Cisco Data Center 実践シリーズ

- Cisco UCS オーバービュー
- Cisco Nexus オーバービュー
- Cisco ACI オーバービュー
- 速習Cisco UCS 実装編
- 速習Cisco Nexus 実装編
- 速習Cisco UCS トラブルシューティング編
- 速習Cisco Nexus トラブルシューティング編
- Cisco Data Center Application Centric Infrastructure v2.0 «DCAC9K»

CCNA Cisco Data Center

- Introducing Cisco Data Center Networking (DCICN) v6
- Introducing Cisco Data Center Technologies (DCICT) v6

CCNP Cisco Data Center

- Implementing Cisco Data Center Infrastructure (DCII) v6
- Implementing Cisco Data Center Unified Computing (DCUCI) v6
- Designing Cisco Data Center Infrastructure (DCID) v6
- Implementing Cisco Data Center Virtualization and Automation (DCVAI) v6
- Troubleshooting Cisco Data Center Infrastructure (DCIT) v6

TRAINOCATE

【トレノケート 共催】

Cisco Support Community Expert Series Webcast

Cisco ACI 入門

日鷹 仁司 (Hitoshi Hidaka)
トレノケート 株式会社
Cisco 認定インストラクター

2018/6/26

投票質問 1

Cisco ACI について、どの程度ご存じでしょうか？

1. 実際に使用している
2. 設定したことがある
3. ひととおり学習したことがある
4. 言葉は聞いたことがある
5. はじめて聞いた

Agenda

1. Cisco ACIの特徴

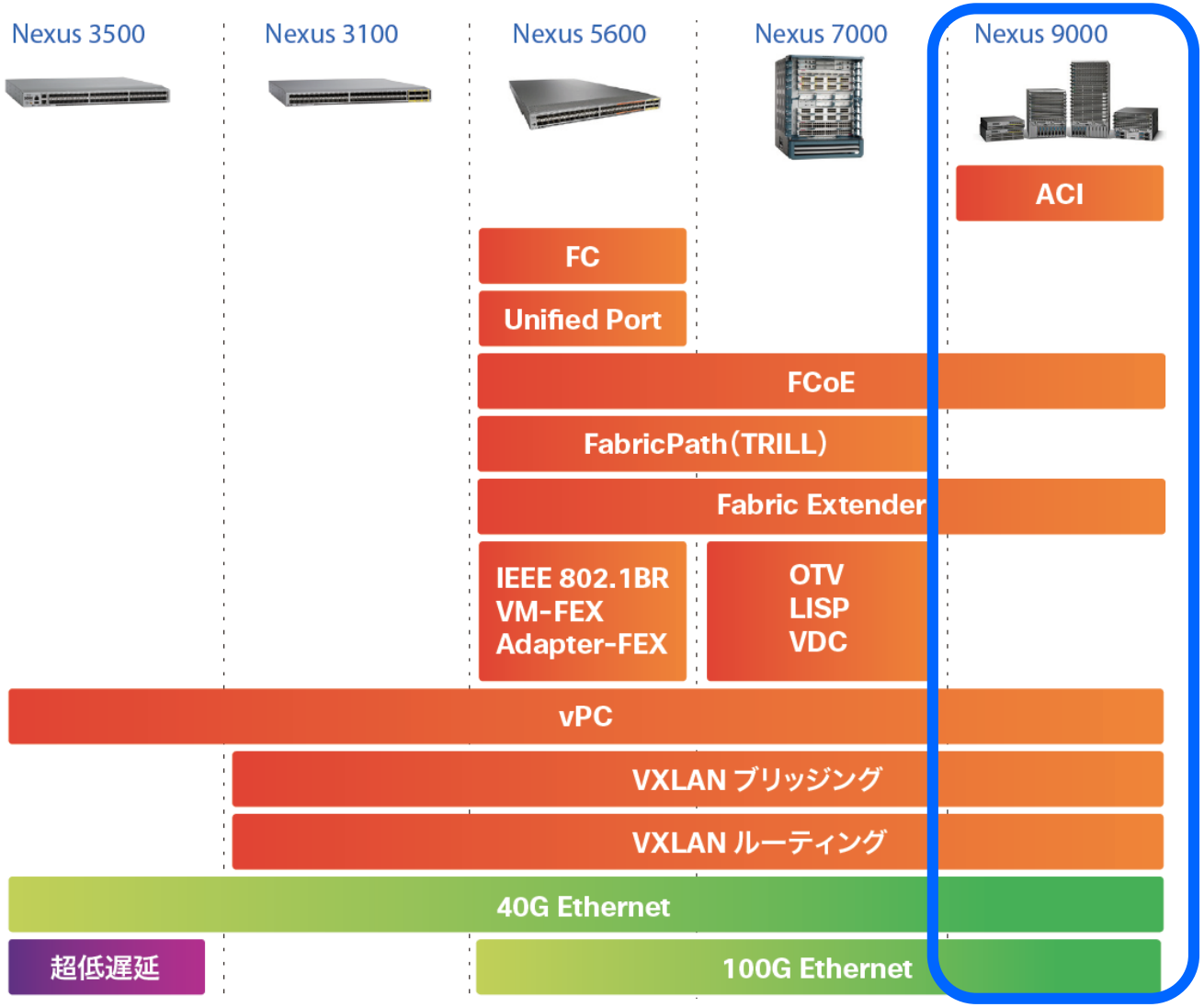
- Cisco ACIのDeployモデル
- Cisco ACIファブリックの基本構成
- APICの役割
- Cisco ACIファブリックの統合オーバーレイ
- 正規化

2. ACIのポリシーモデル

- ACIのポリシー
- テナントとコンテキスト
- Bridge DomainとEPG
- コントラクトとApplication Profile
- アクセスポリシー
- ACIへのサービス挿入
- 外部ネットワークとの接続

Cisco ACI の特徴

Cisco Nexus 9000 シリーズスイッチの特徴



NX-OSモードとACIモード

NX-OSモード

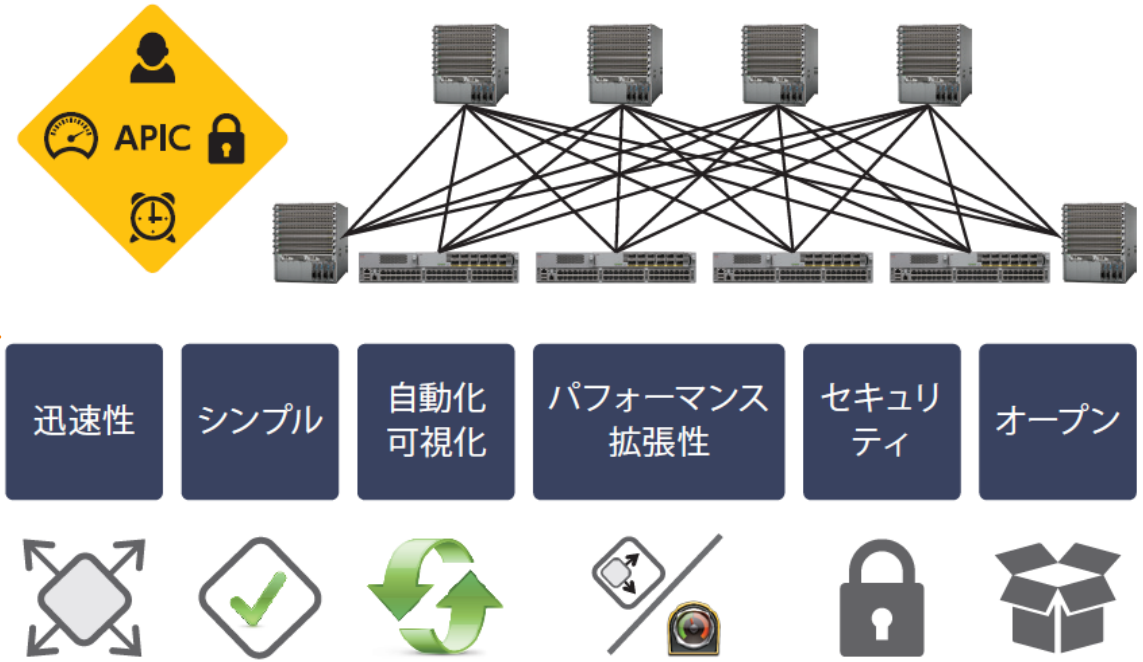
Cisco Nexus 9000シリーズ

- 1/10/40/100GbE対応
- VXLAN/プログラマビリティ
- DevOps/低価格/省電力

次世代インフラのベース

ソフトウェア
アップグレード
ACIへの移行

ACIモード



迅速性 | シンプル | 自動化 可視化 | パフォーマンス 拡張性 | セキュリティ | オープン

アプリケーション中心のネットワーク

Cisco ACIの特徴

ACIエコシステム
パートナー

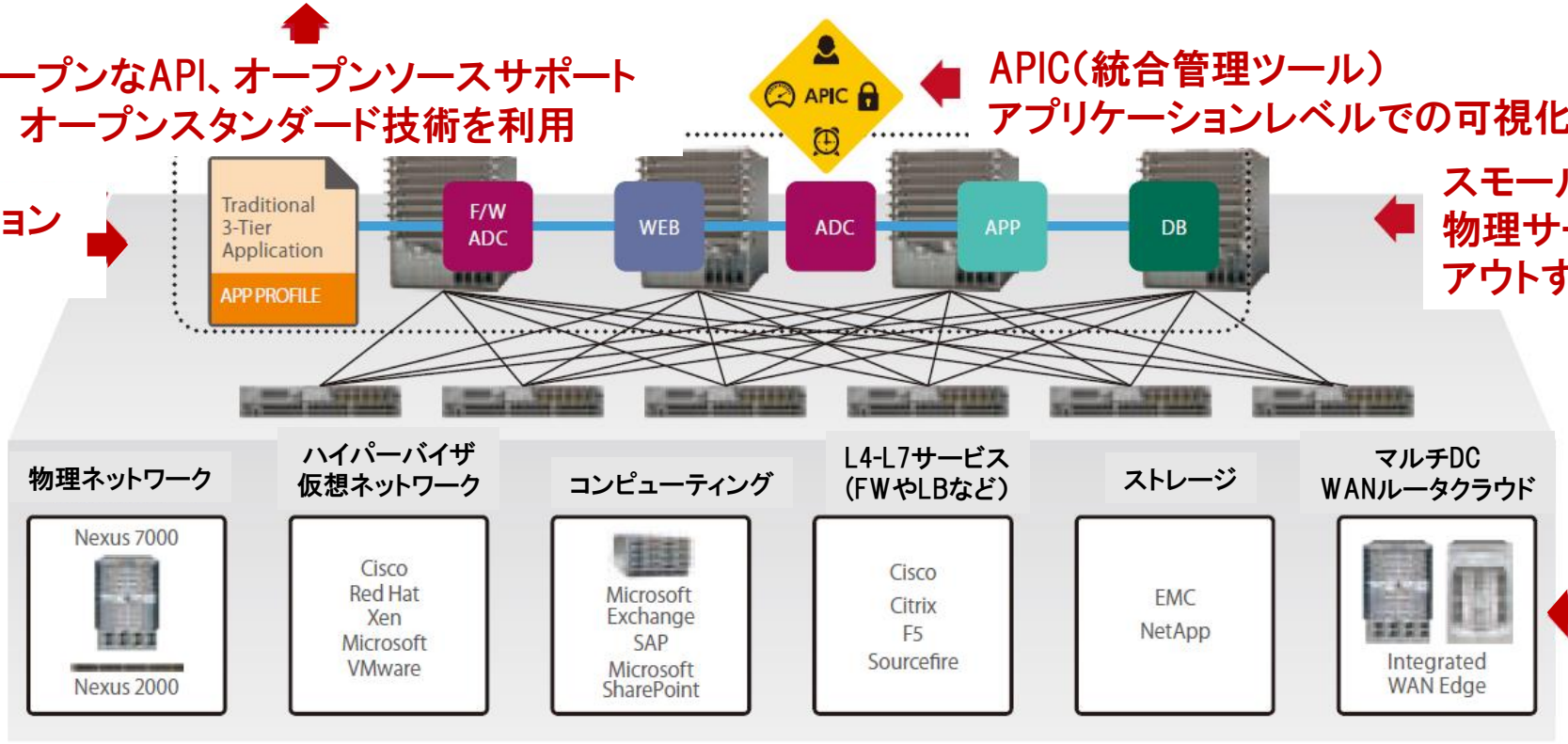
自動化	ハイパーバーザ管理	モニタリング	管理	オーケストレーション
CFEngine, Python Puppet Opsode	Red Hat, Oracle VMware, Xen Microsoft	CA, Net Qos, Splunk OpenStack, NetScout Emulex, IBM	Cisco UCS Director OpenStack, VMware CloudStack, Red Hat	IBM, BMC HP, CA

オープンなAPI、オープンソースサポート
オープンスタンダード技術を利用

APIC(統合管理ツール)
アプリケーションレベルでの可視化

アプリケーション
プロファイル

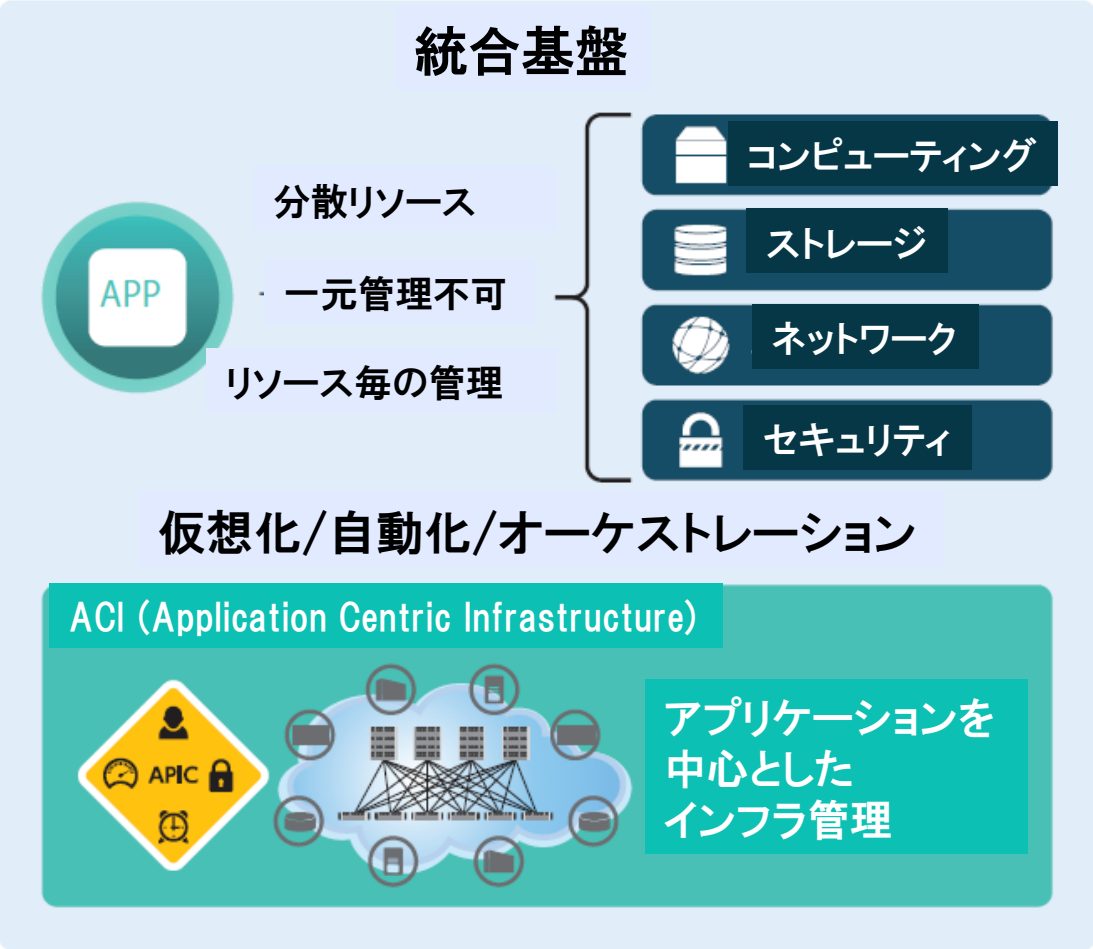
スモールスタートから5万
物理サーバまでスケール
アウトするACIファブリック



マルチハイパー
バイザ＋ベアメ
タルサーバ

TRAINOCATE

Cisco ACIの特徴（続き）



今までのIT基盤の課題

- インフラDeployに時間がかかる
- 管理が分割（サーバ、ネットワーク、ハイパーバイザ）

ACIで実現すること

- アプリ視点のネットワーク管理
- インフラDeploy時間の短縮化
- 運用コストの削減
- 設定ミス、リスクの低減

Cisco ACIの特徴（続き）

物理ネットワーク

Nexus 7000

Nexus 2000

ハイパーバイザ
仮想ネットワーク

Cisco
RedHat
Xen
Microsoft
VMware

コンピューティング

L4-L7サービス
（FWやLBなど）

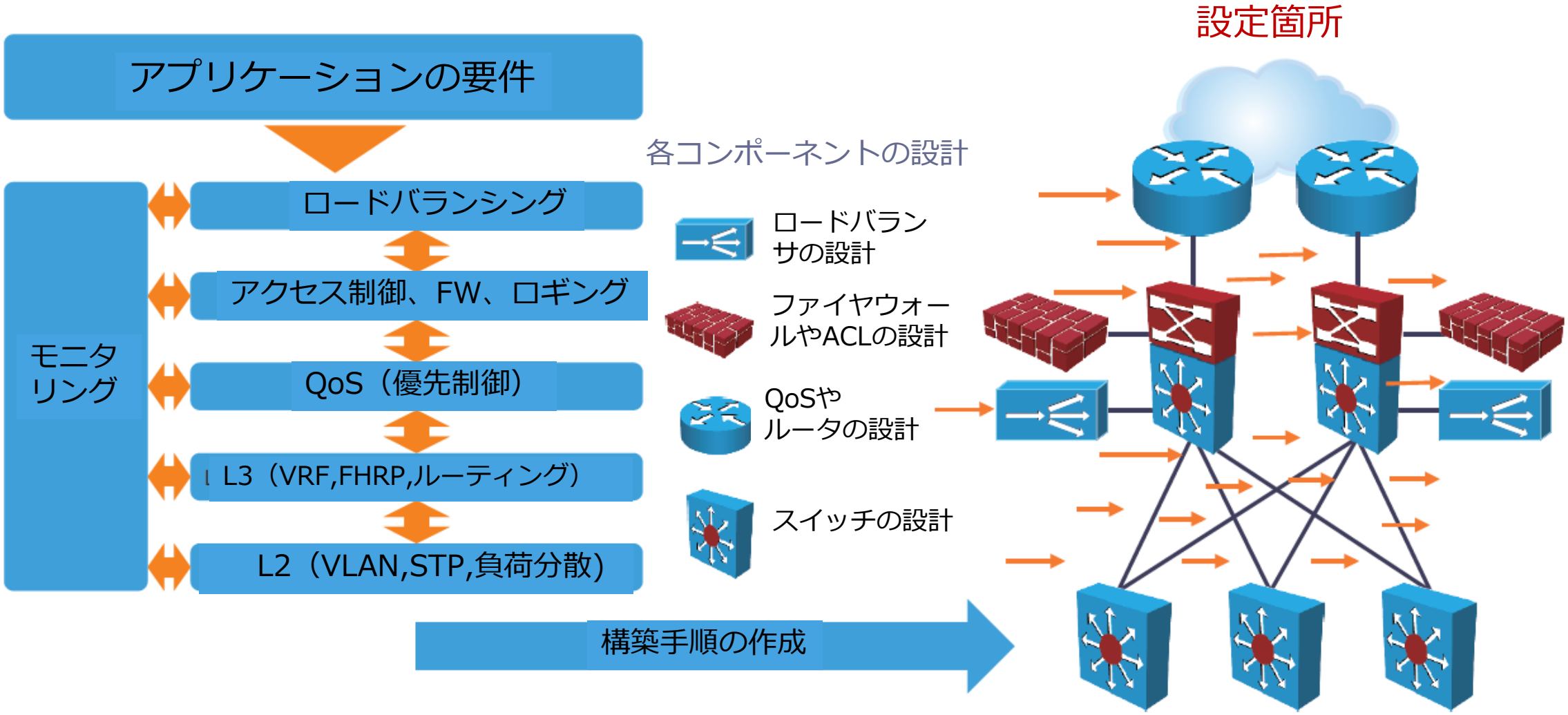
Cisco
Citrix
F5
Sourcefire

ストレージ

マルチDC
WANルータ
クラウド

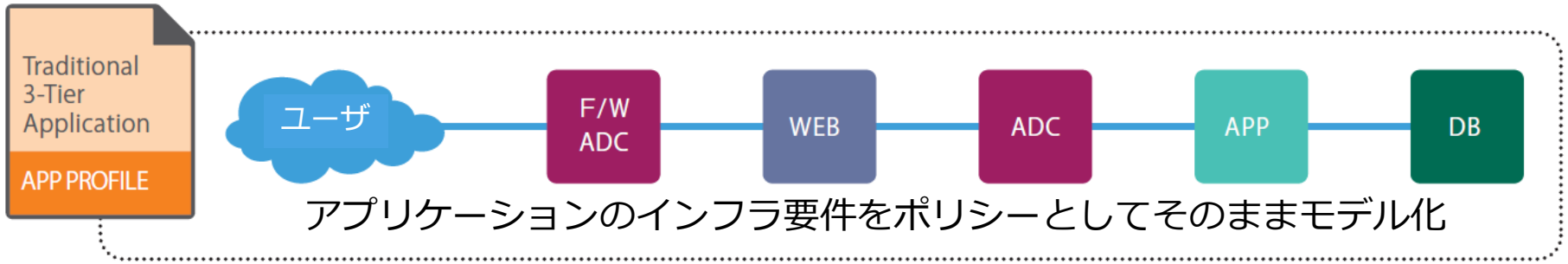
Integrated
WAN Edge

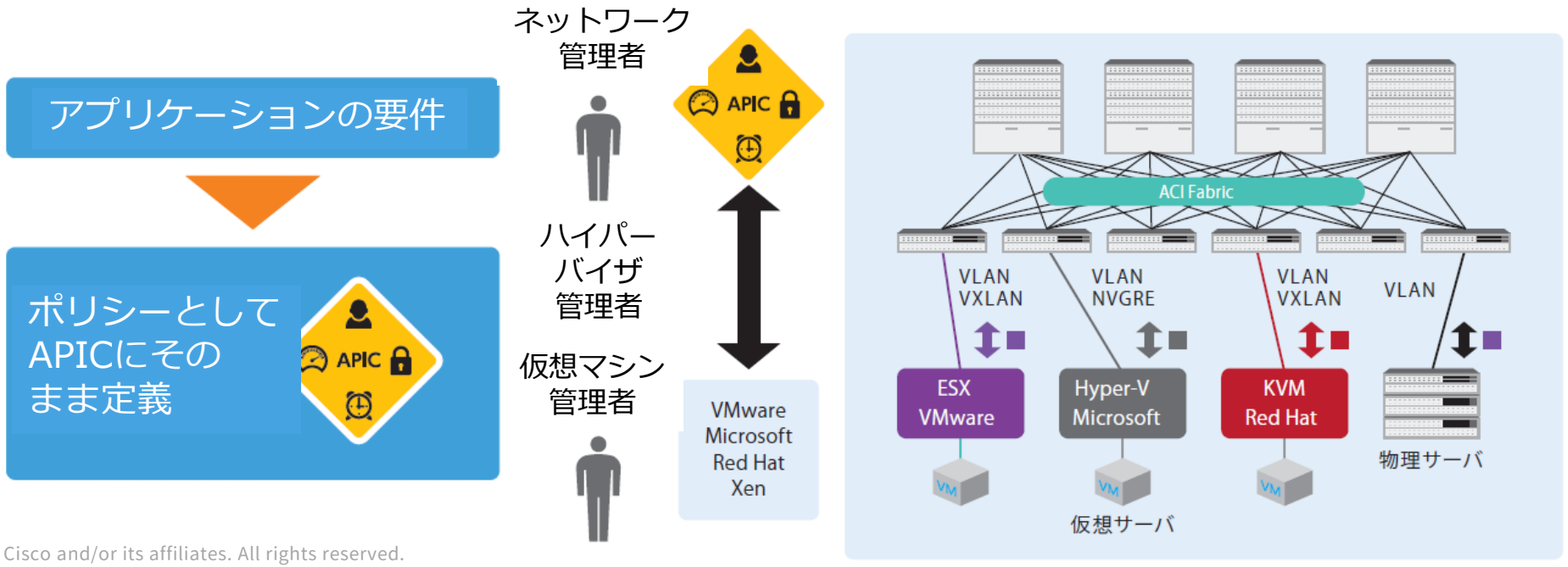
従来のネットワークのDeployにおける課題



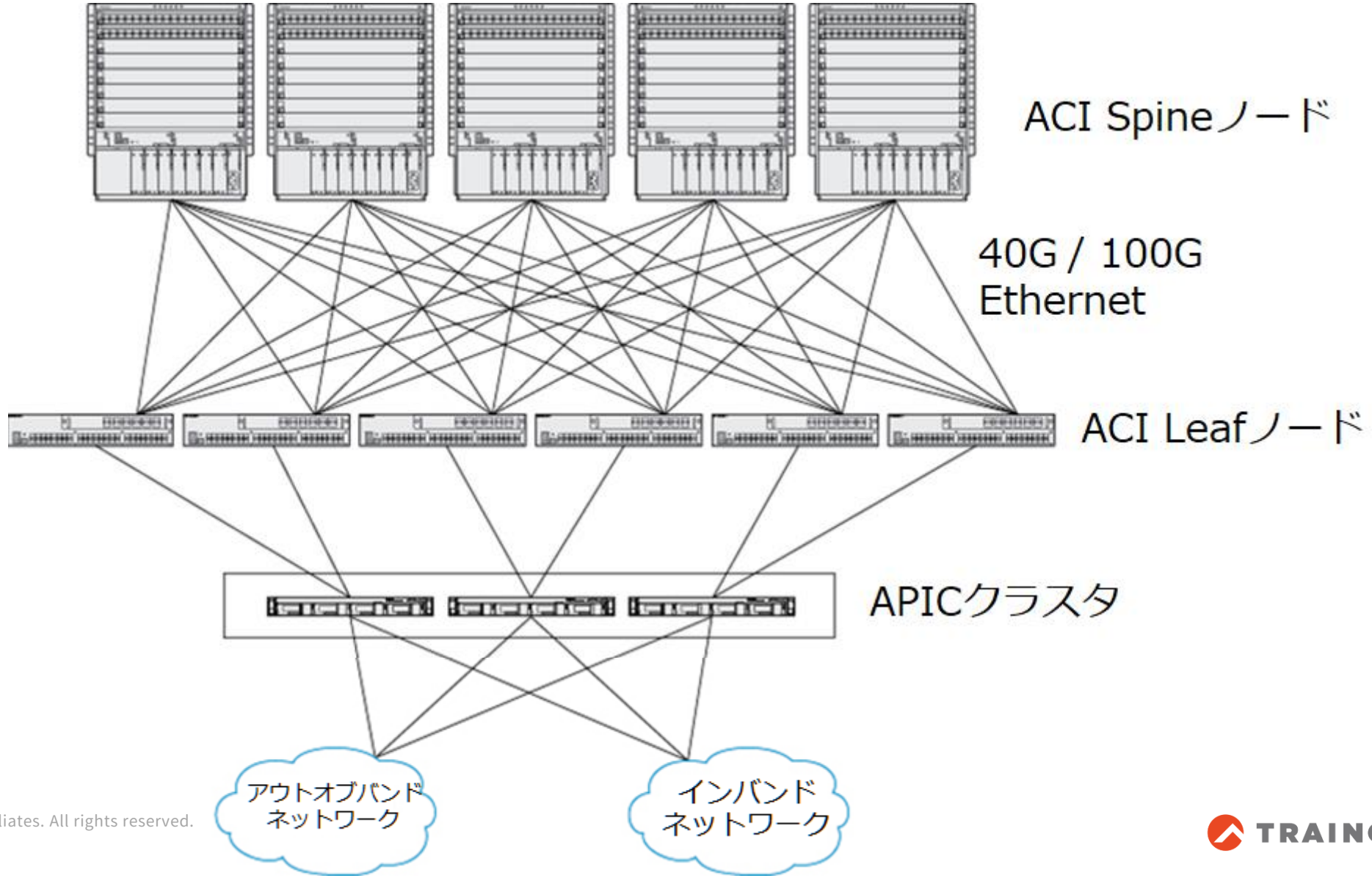
TRAINOCATE

ACIのDeployモデル

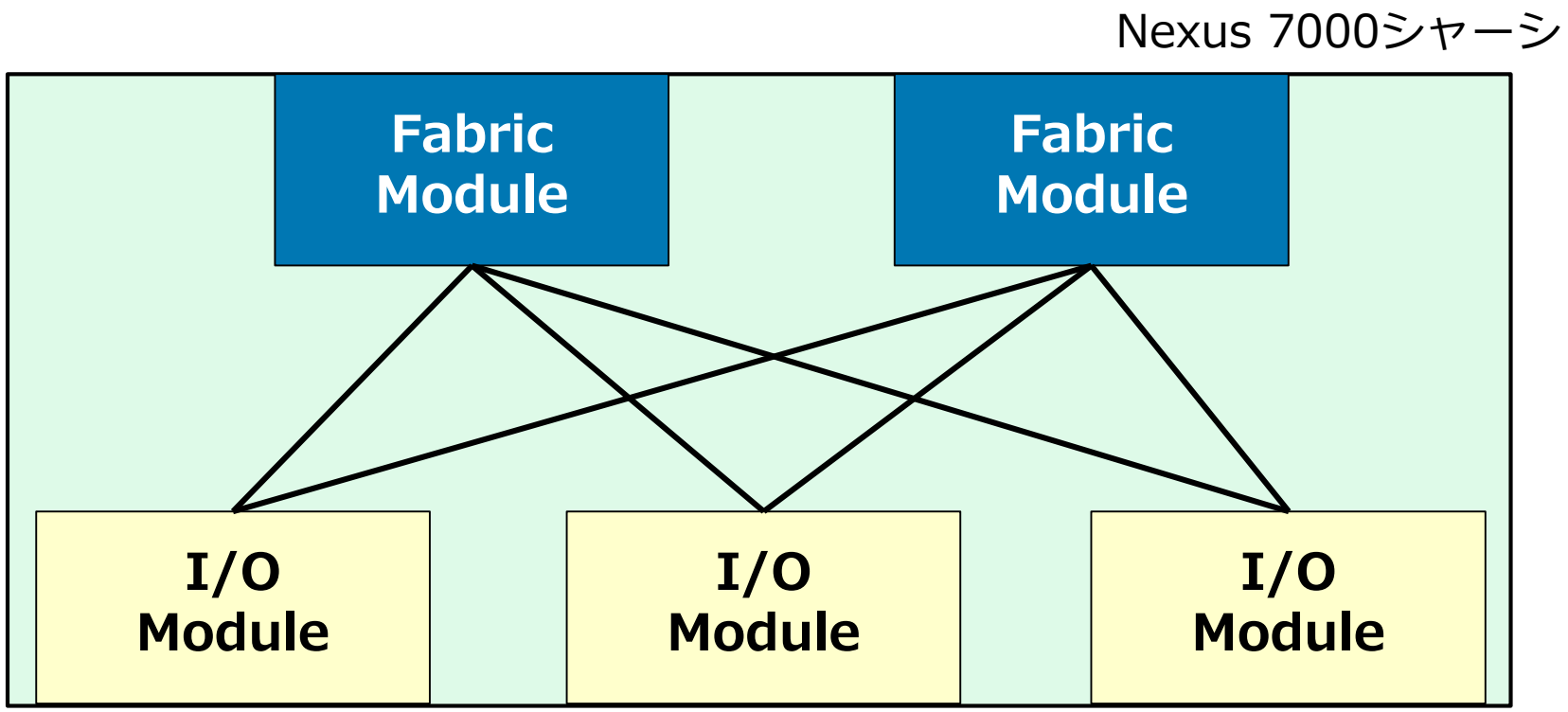




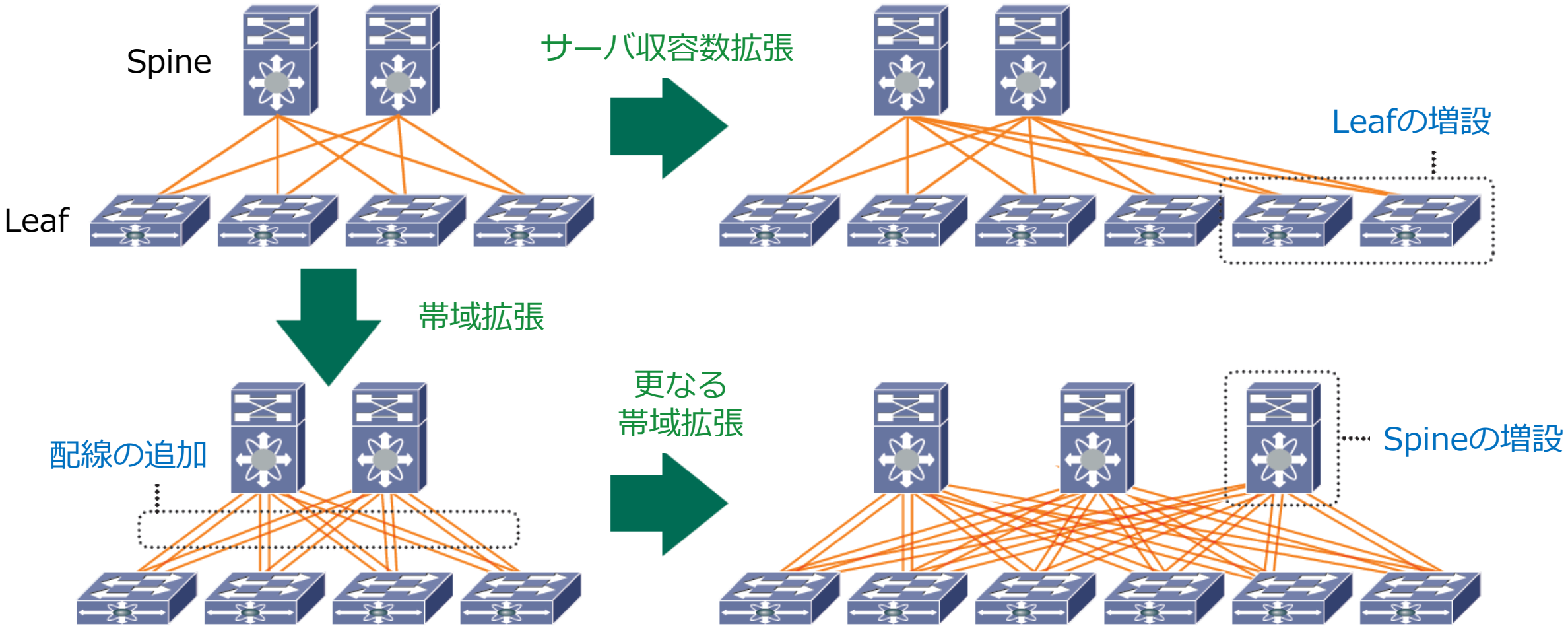
ACIファブリックの基本構成



参考：Nexus 7000のFabric ModuleとI/O Module



ファブリックのスケールアウト



APIC (Application Policy Infrastructure Controller)

物理ネットワーク

ハイパーバイザ
仮想ネットワーク

Cisco
RedHat
Xen
Microsoft
VMware

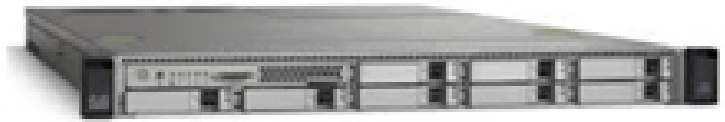
コンピューティング

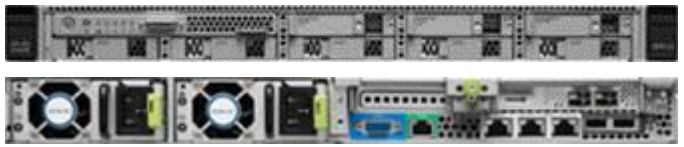
L4-L7サービス
(FWやLBなど)

Cisco
Citrix
F5
Sourcefire

ストレージ

マルチDC
WANルータ
クラウド



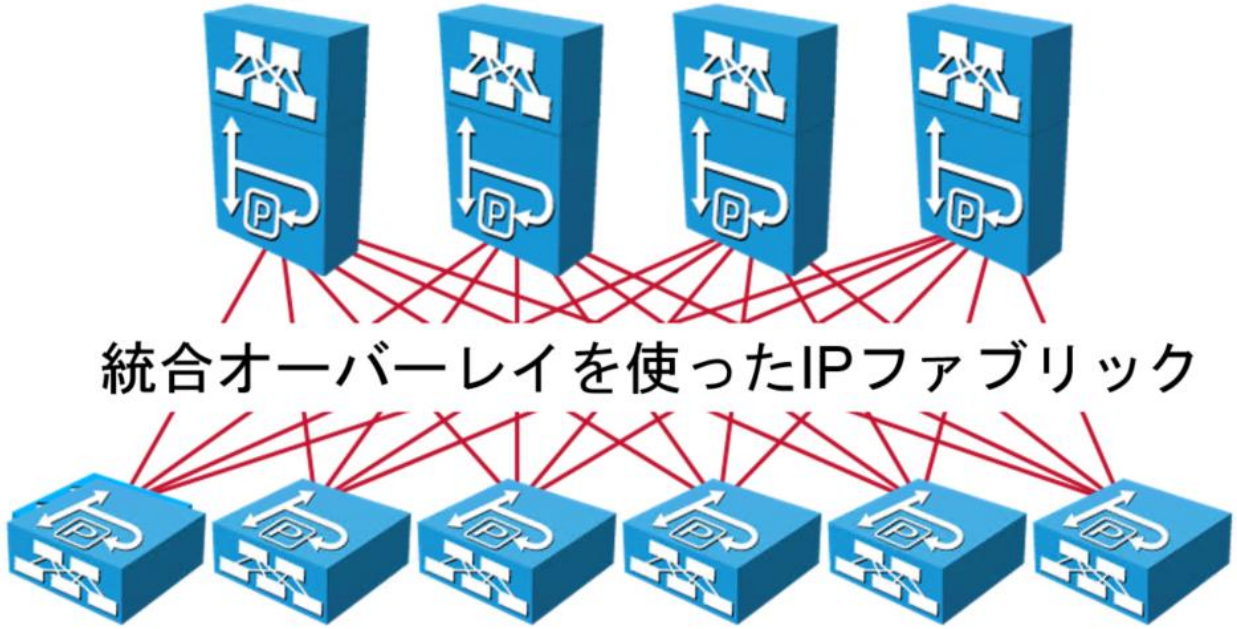


Medium	APIC-CLUSTER-M1	中規模向け(最大1000エッジポート)
Leage	APIC-CLUSTER-L1	大規模向け(1000以上のエッジポート)

APICの役割

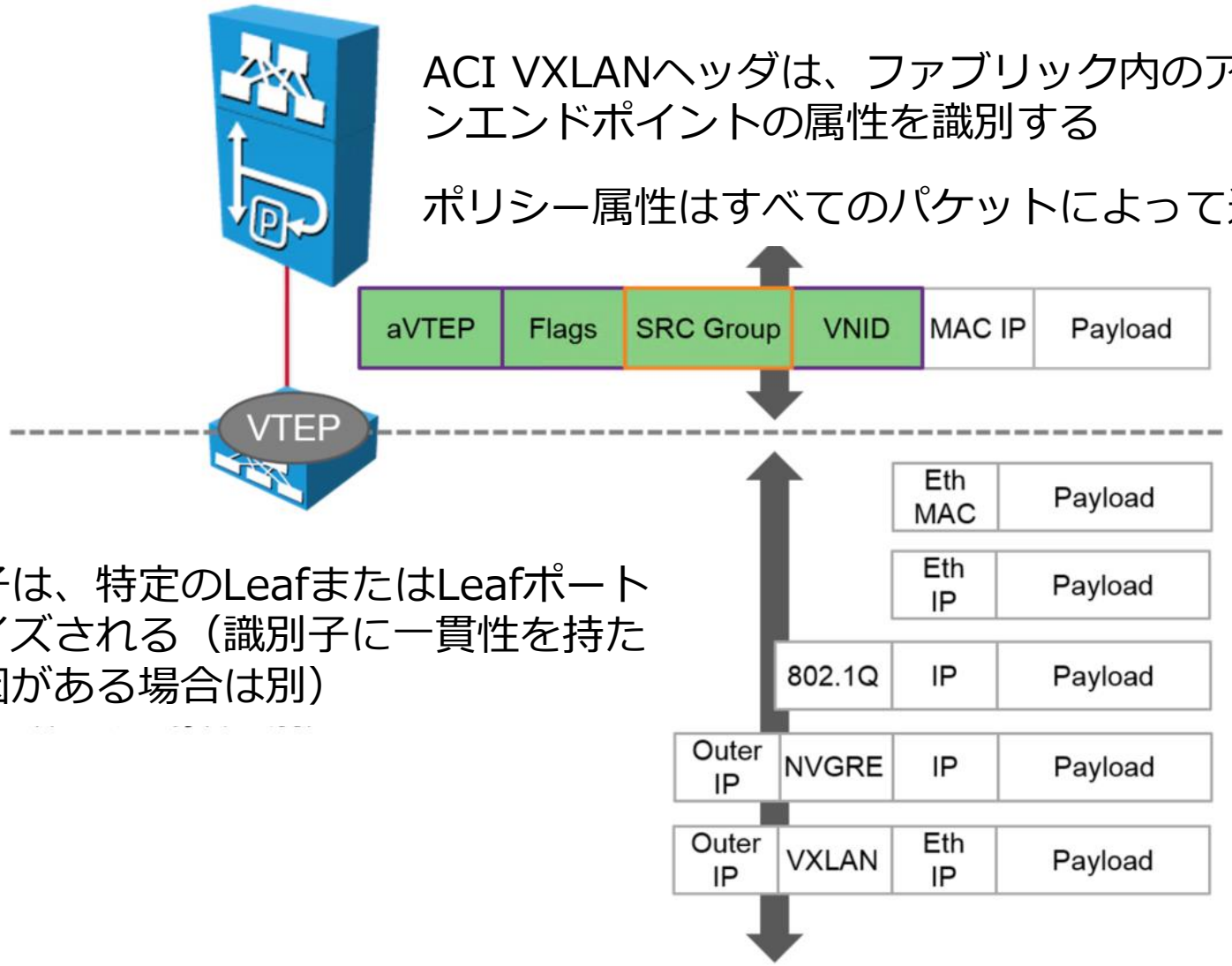
- ポリシーコントローラ
- 定義済みポリシーを保持
- 定義、変更したポリシーをインスタンス化する
- 最低3台以上のサーバで高度に冗長化したクラスタを構成する
- コントロールプレーンではない
- APICはトラフィックパス上には存在していない

Spine-Leafシングルサイト トポロジ



- 40-Gb IPファブリック（100Gbにも対応）
- 最少2台のSpine（1 + 1 冗長）
- Leaf スイッチ同士やSpineスイッチ同士は接続しない
- Leafスイッチにはエンドデバイス（サーバ）やL4-L7デバイス（ファイヤウォールやロードバランサ）、外部ネットワークへ接続するL2/L3機器を接続する

Cisco ACIファブリックの統合オーバーレイ



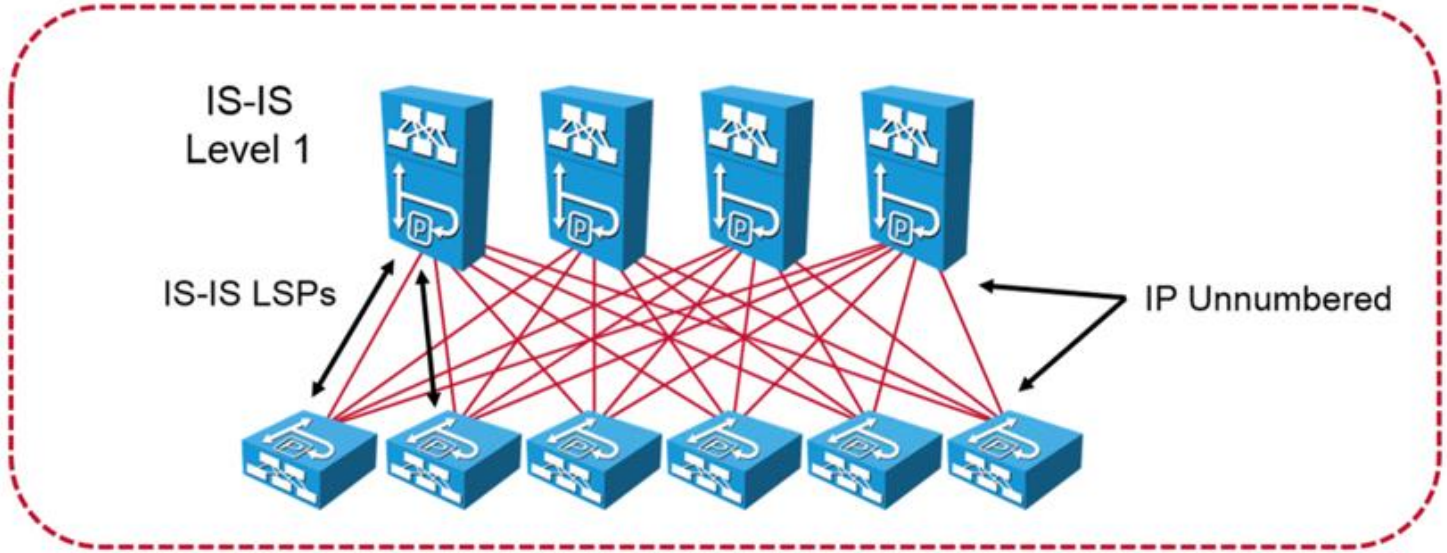
ACI VXLANヘッダは、ファブリック内のアプリケーションエンドポイントの属性を識別する

ポリシー属性はすべてのパケットによって運ばれる

外部の識別子は、特定のLeafまたはLeafポートにローカライズされる（識別子に一貫性を持たせる外部要因がある場合は別）

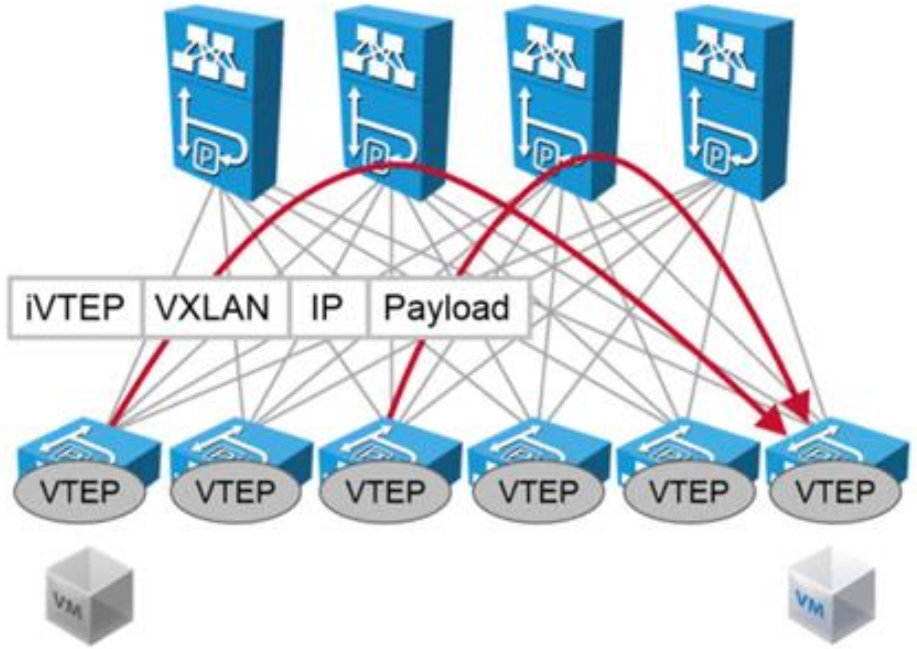
IS-ISファブリック インフラストラクチャ ルーティング

- ファブリックは、インフラストラクチャトポロジ形成にIS-ISを活用
- LoopbackとVTEPアドレスの広報
- ベンダTLVを使って、ファブリック内にマルチキャストFtagツリーを生成する
- IS-ISは各TEP（トンネルエンドポイント）を識別し、各Leafノードからファブリック内の他のすべてのノードへトンネル形成を通知する
- IS-ISはACIファブリックに合わせてチューニングされている

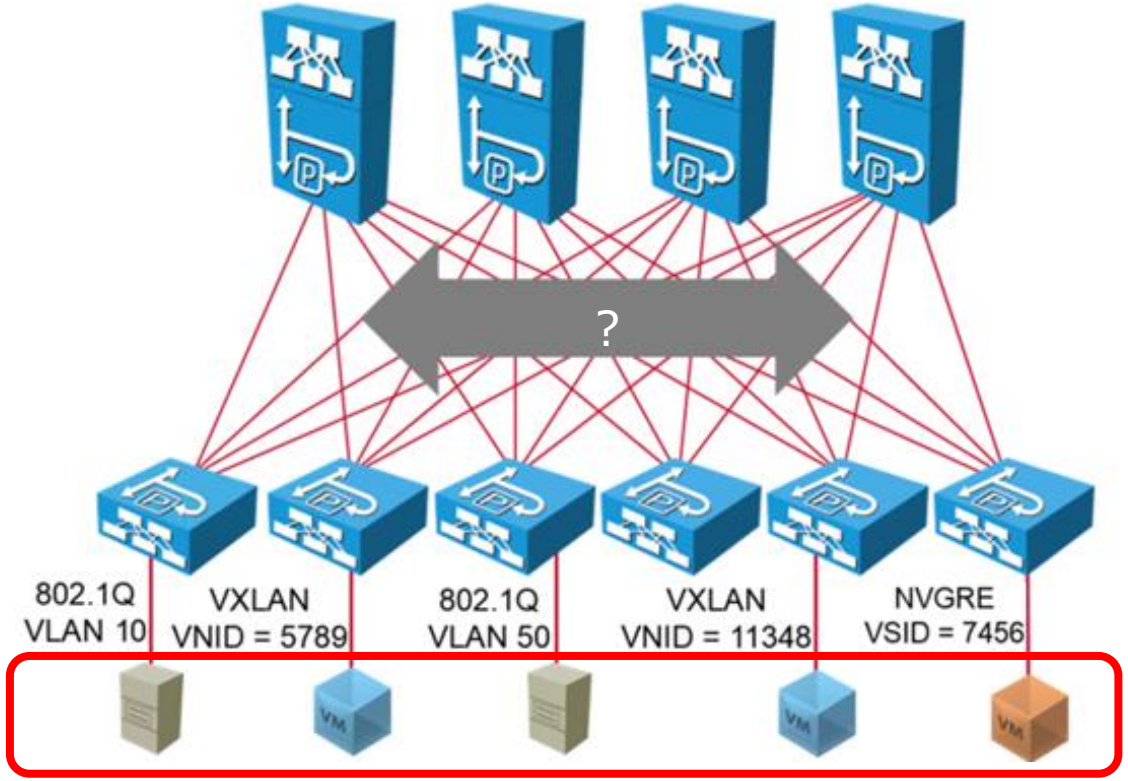


識別子、場所、ポリシーの切り離し

- ACIファブリックは、ロケータやVTEPアドレスに定義されているエンドポイントの場所情報を、その識別子であるエンドポイントアドレスから切り離す
- ファブリック内においてVTEP間に転送されるパケットは、拡張VXLANヘッダを用いる
- 内部テナントのMACアドレスやIPアドレスと位置情報のマッピングは、各VTEPによって分散マッピング（到達可能性）データベースを使用して実行される



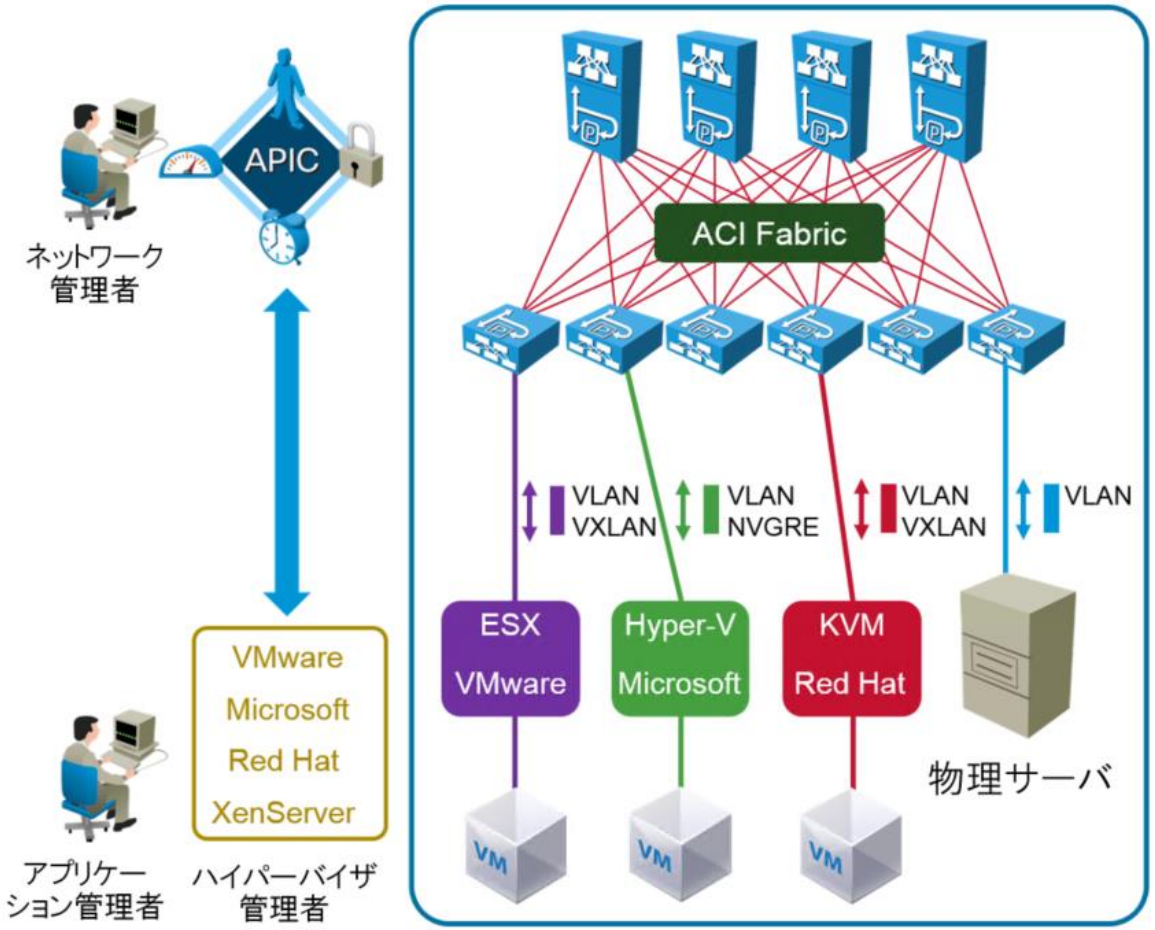
投票質問 2



上記サーバ間の通信性の説明で正しいものはどれでしょうか？

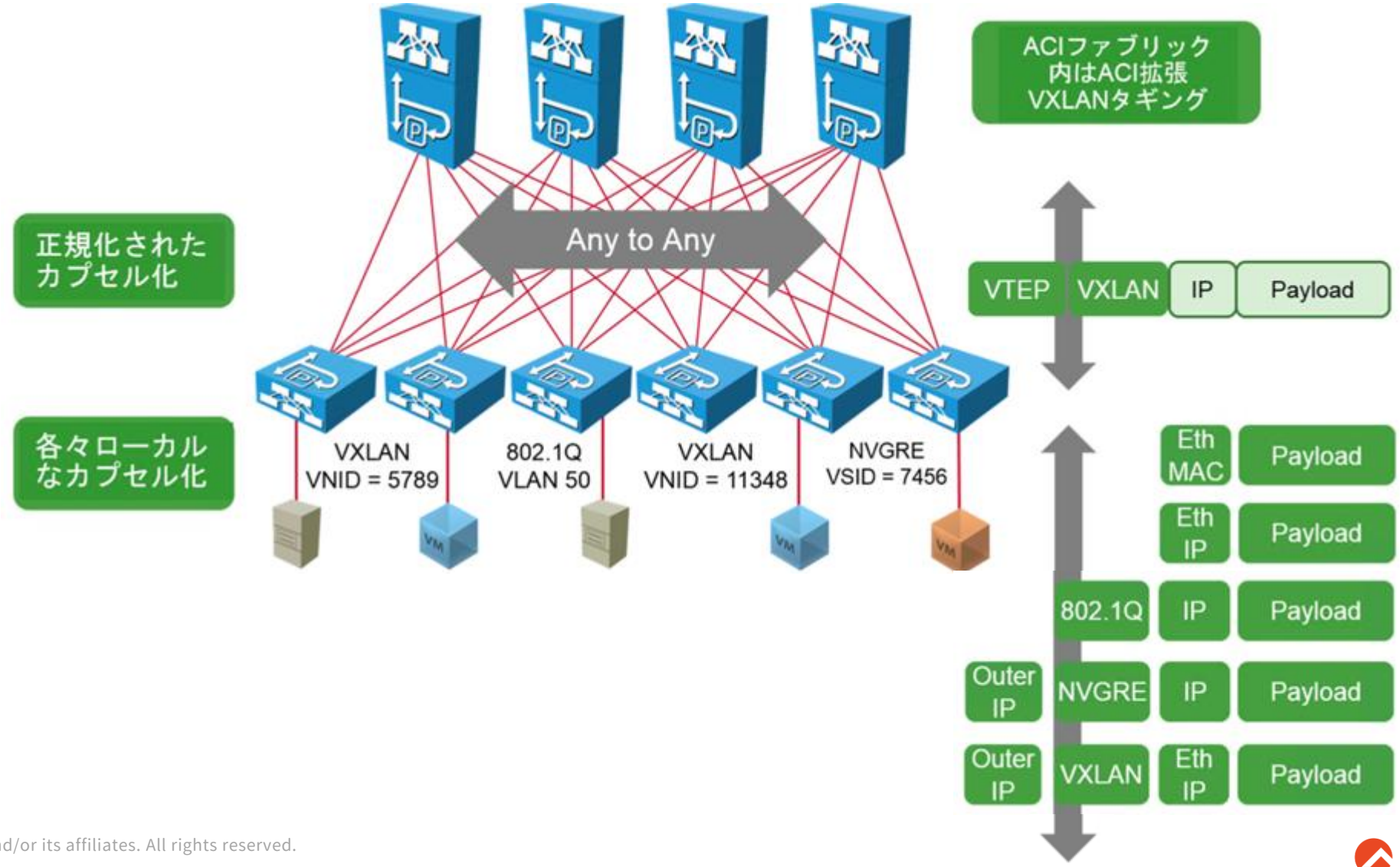
1. VLAN同士、VXLAN同士はルーティング可能だが、それ以外は通信できない
2. VLAN-VXLAN間、VLAN-NVGRE間は相互通信は可能だが、NVGRE – VXLAN間の通信はできない
3. ACIポリシーを設定すれば、Any to Anyで通信可能

マルチハイパーバイザにおける正規化（Normalization）



- Leafスイッチは、仮想から物理へのVLAN、VXLAN、およびNVGREネットワーク用の統合ゲートウェイとして機能する
- VLAN、VXLAN、およびNVGREネットワークを内部のACI VXLANに正規化する
- ACIに接続するハイパーバイザの制限はない（混在しても相互通信可能）

正規化によるAny to Any通信



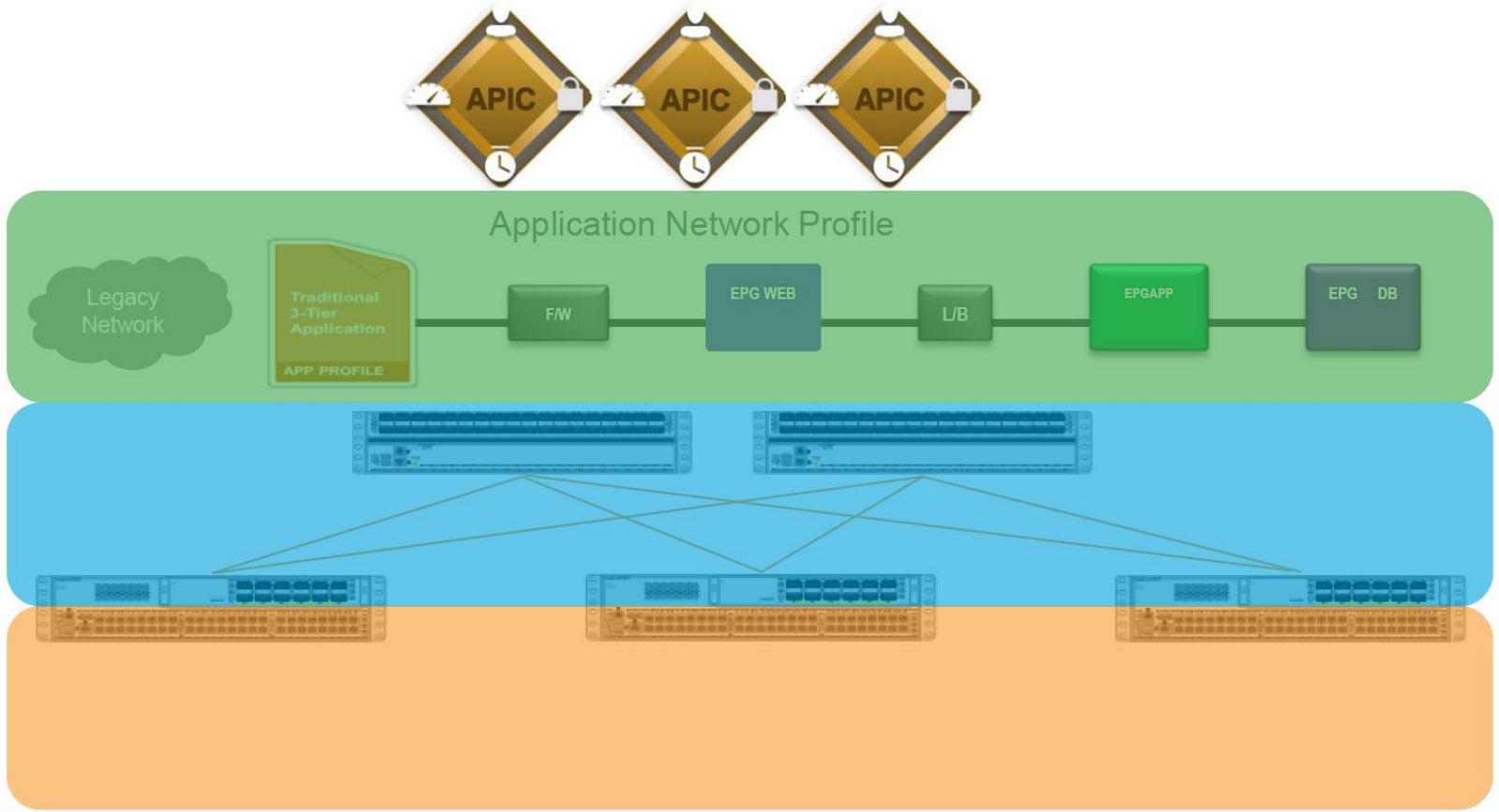
Cisco ACI ポリシーモデル

ACIのポリシー

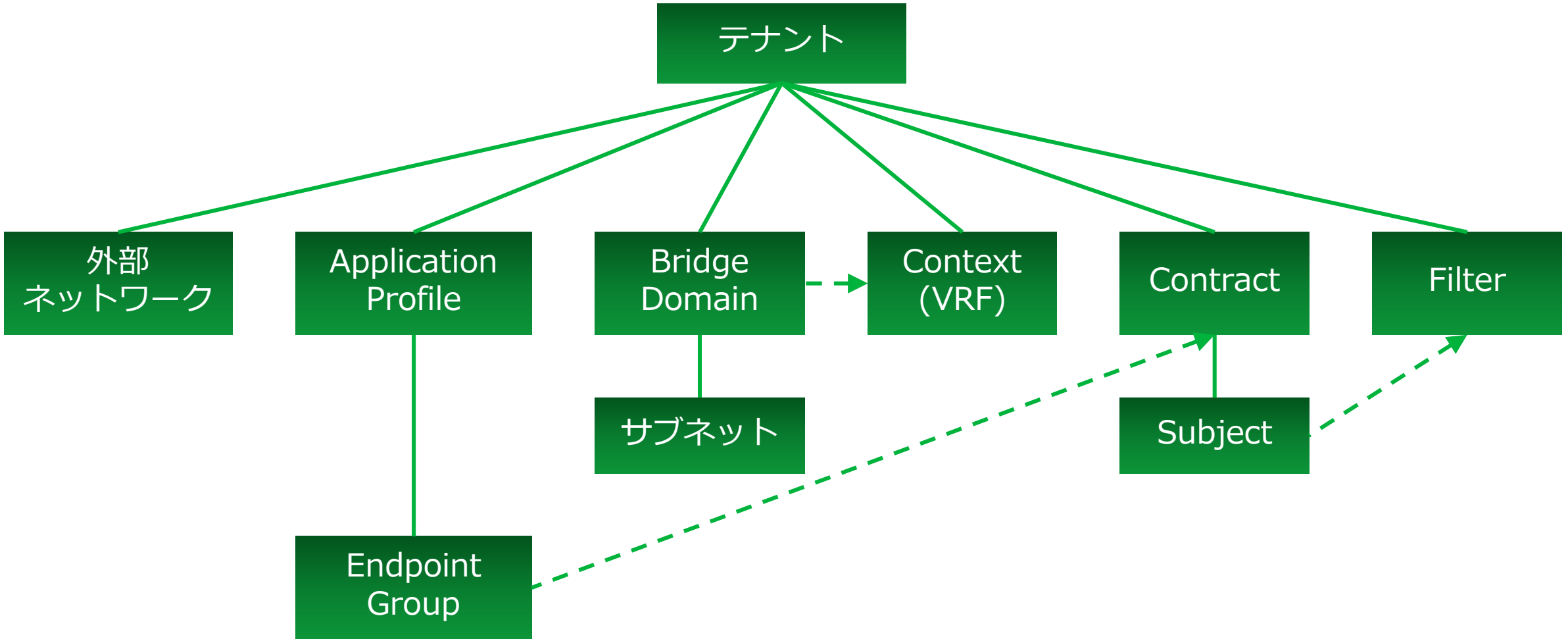
テナント ポリシー

ファブリック ポリシー

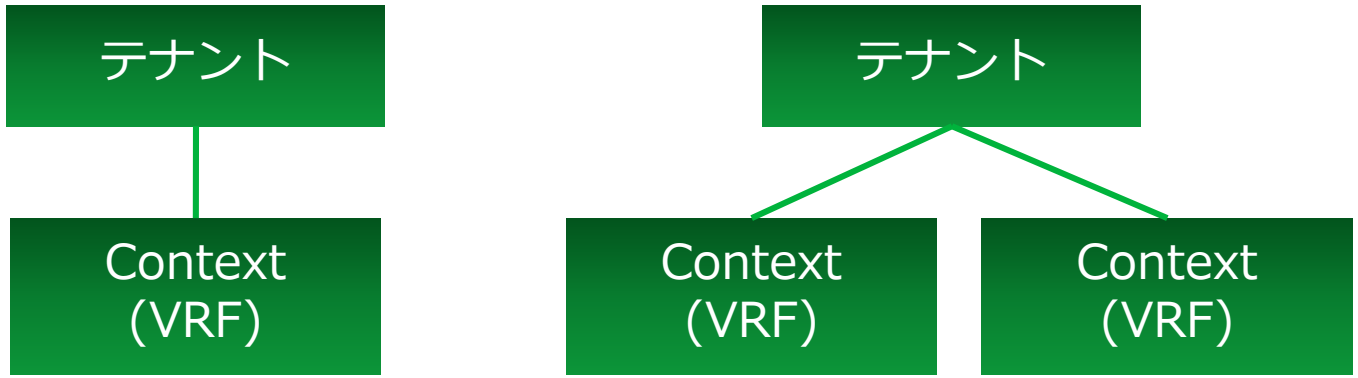
アクセス ポリシー



テナントモデルの全体像



テナントとContext



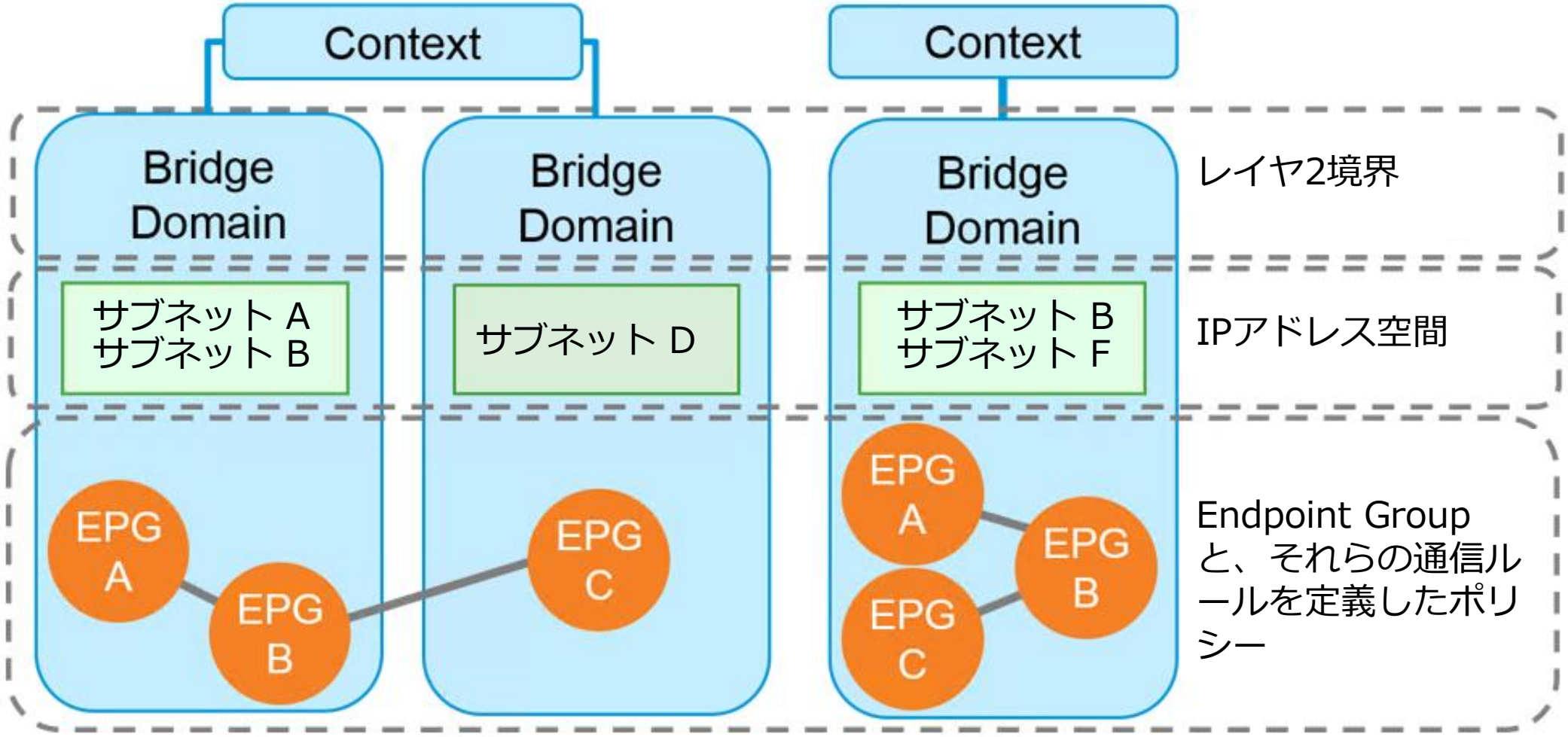
テナント

- 顧客、部門、グループなど
- テナントごとに異なるポリシー
- 他のテナントは基本的には参照できない
- 複数のテナントで共有するサービスを作成可能

Context

- Contextはレイヤ3ルーティングドメイン
- Contextごとにルーティング、通信は基本的に独立している
- IP空間の再利用（Contextごとに重複してもよい）

Bridge Domain

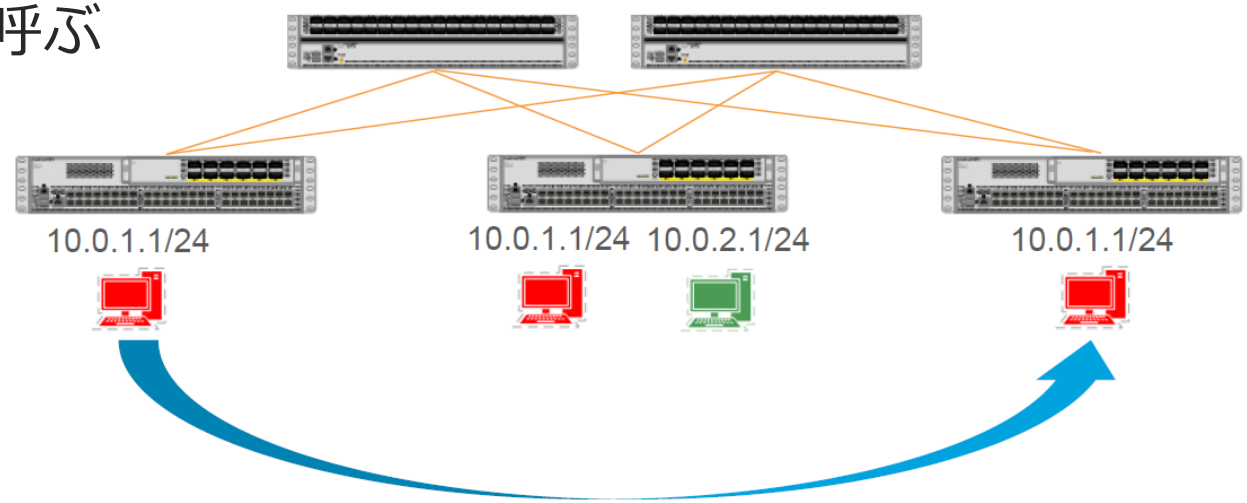


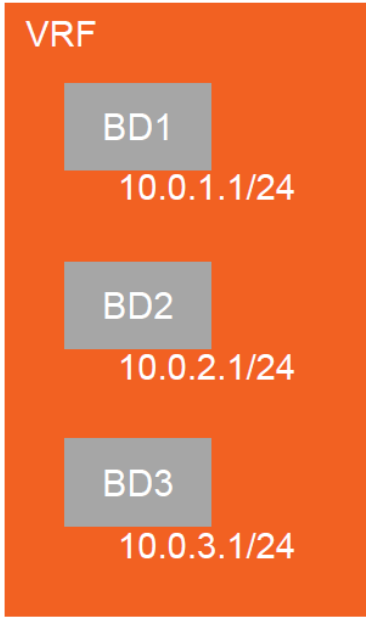
Bridge Domainの特性

- レイヤ2境界としての動作は設定で変更可能
  - L2 Unknown Unicast (Flood | Hardware Proxy)
    - Hardware Proxyにした場合、Unknown UnicastのアドレスがSpineのProxy Station Tableになければ破棄される
  - L3 Unknown Multicast (Flood | Optimized Flood)
    - Optimized Foodは同じBDのルータポートにのみフラッドされる
  - Multi-Destination Flooding (Flood in BD | Drop | Flood in Encapsulation)
    - マルチキャストフレームの転送
    - Flood in Encapsulationの場合、同じBridge Domainの同じVLANなどの設定ポートにのみフラッドされる。Flood in BDの場合、Bridge Domainのすべてのポートへフラッドされる
  - ARP Flooding (On | Off)
    - ARP Requestをフラッドするか否か

サブネットの取り扱い

- BDにサブネットを定義すると、Endpointが所属するスイッチにだけSVIが作成される
- Pervasive Gatewayと呼ぶ



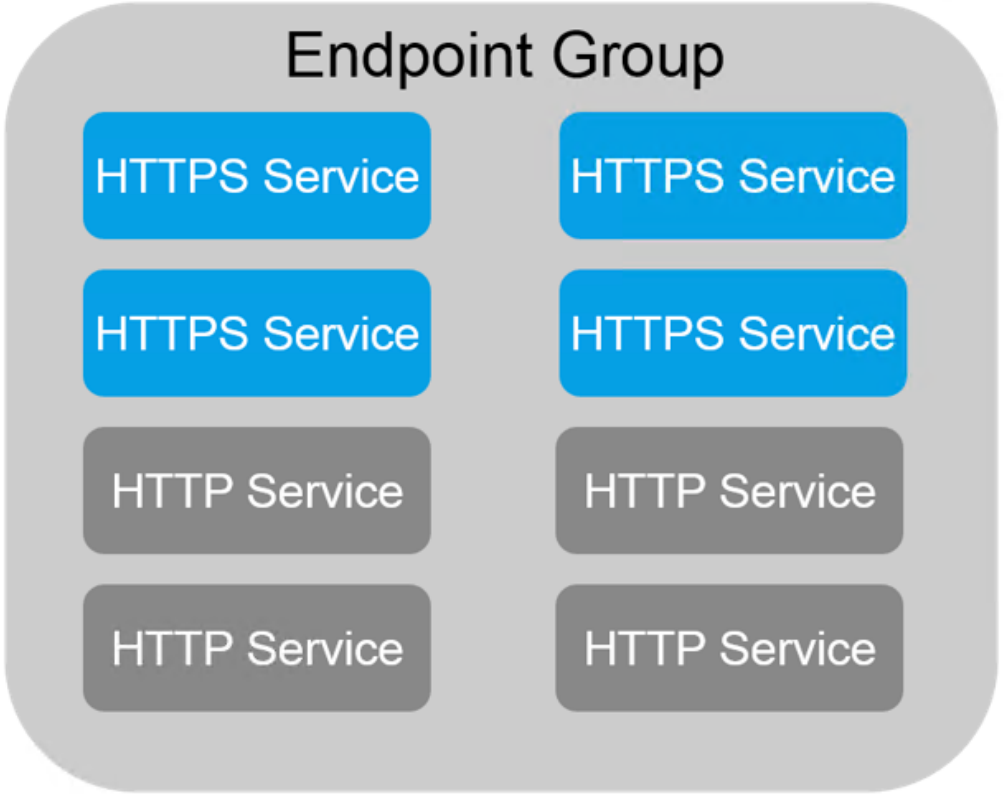


- エンドポイントが移動すると、移動前のLeafポートからSVIは削除され、新しいLeafポートにプログラムされる
- ゲートウェイは常に1ホップ。識別と位置を切り離す
- 同じVRF内のすべてのBDルートは自動的に把握するので、ACIファブリック内でのルーティングプロトコルの設定は不要

Endpoint Group

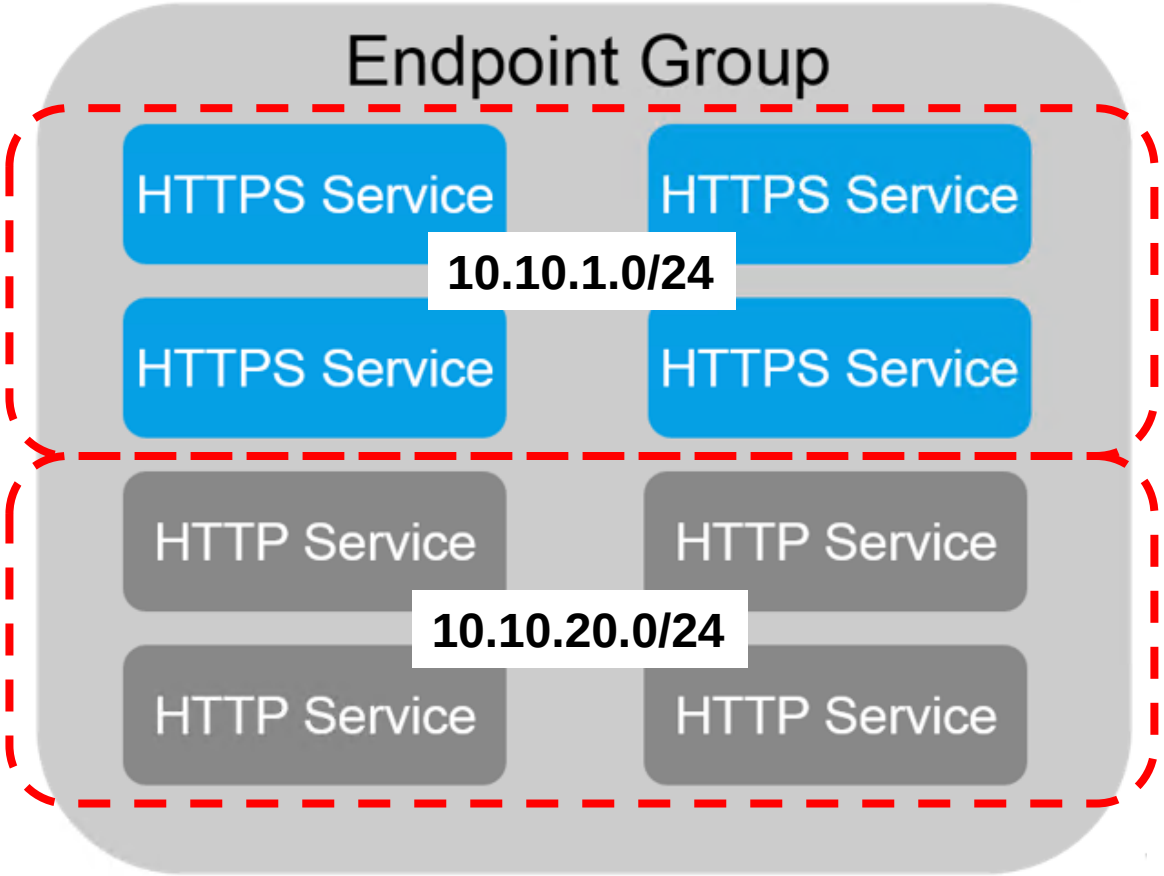
- Endpoint Groupはアプリケーションやアプリケーションコンポーネントのグループで、他の構成要素から独立している

- マイクロセグメンテーションの設定をしない限り、Endpoint Group内の通信は自由に行うことができる

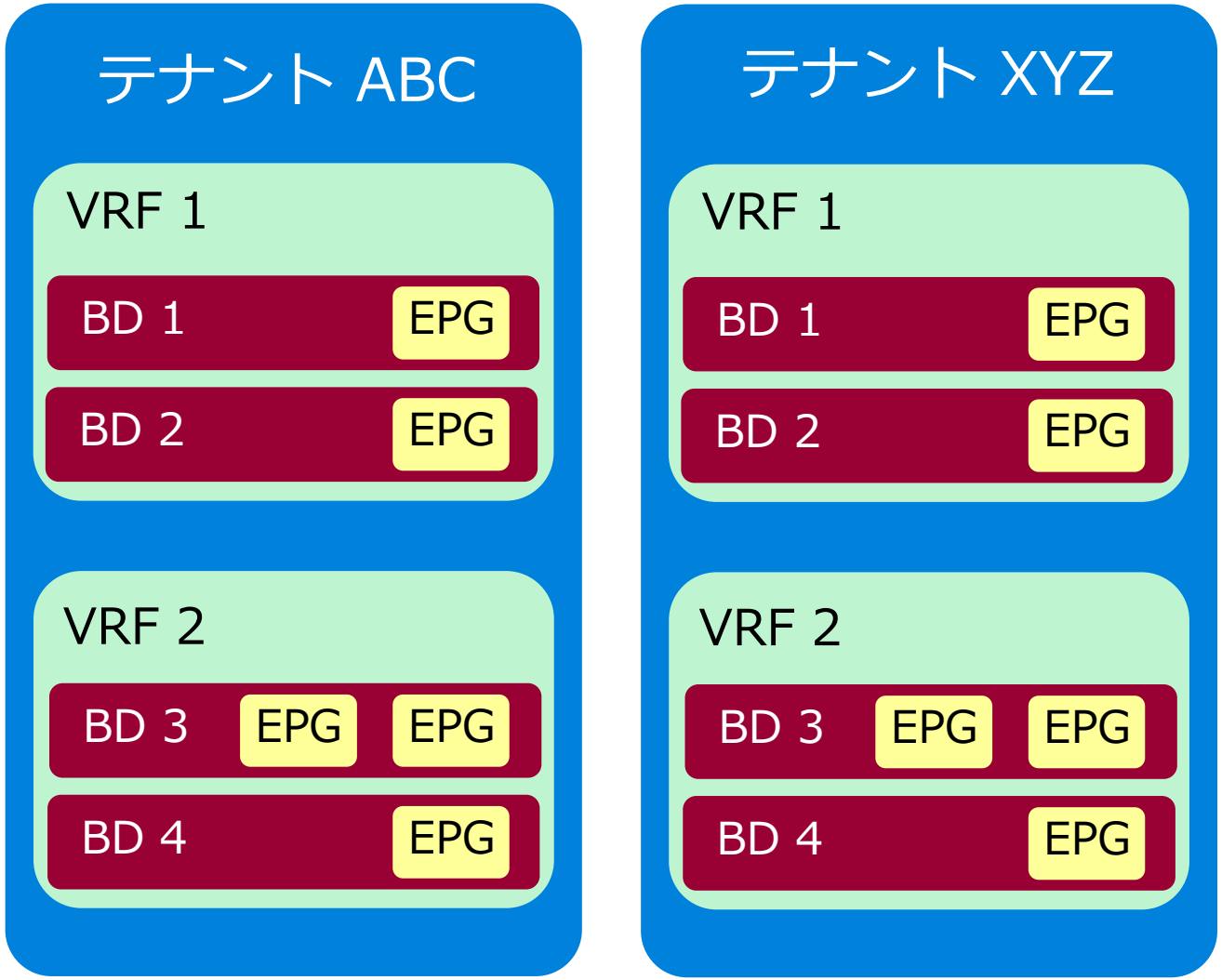


Endpoint Group（続き）

- Endpoint Groupは、IPアドレス（サブネット）とは関係なく設定できる
- 通信セキュリティのポリシーを同一に扱うべきものをメンバに入れる
- ポリシーとセキュリティはEPG間の通信に対して設定



Endpoint Group（続き）



EPGは単一のBridge Domainに所属する

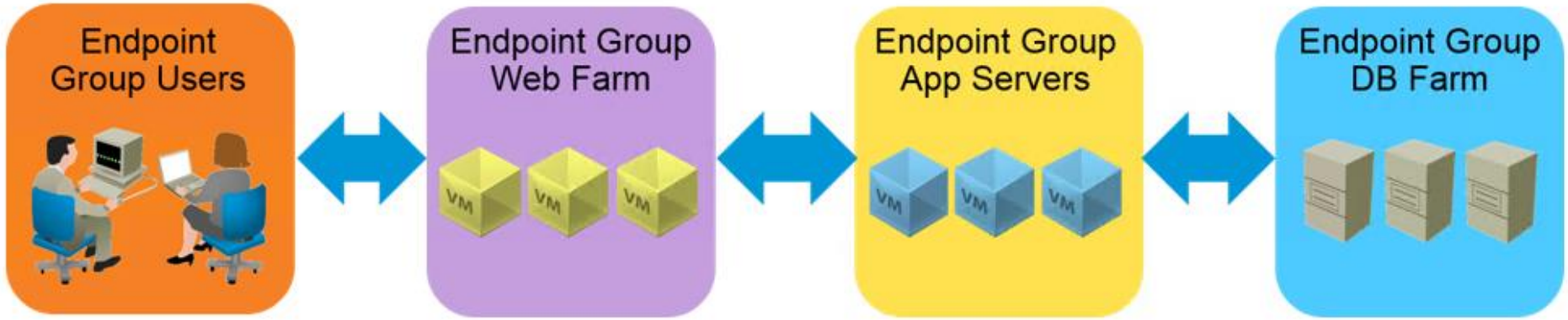
複数のBridge Domainにまたがるは存在しない

Endpoint

- 物理設定や仮想設定と紐づけることができる
  - ACIファブリック、Leafノードの物理ポート
  - MACアドレス
  - VLAN
  - VMwareポートグループ

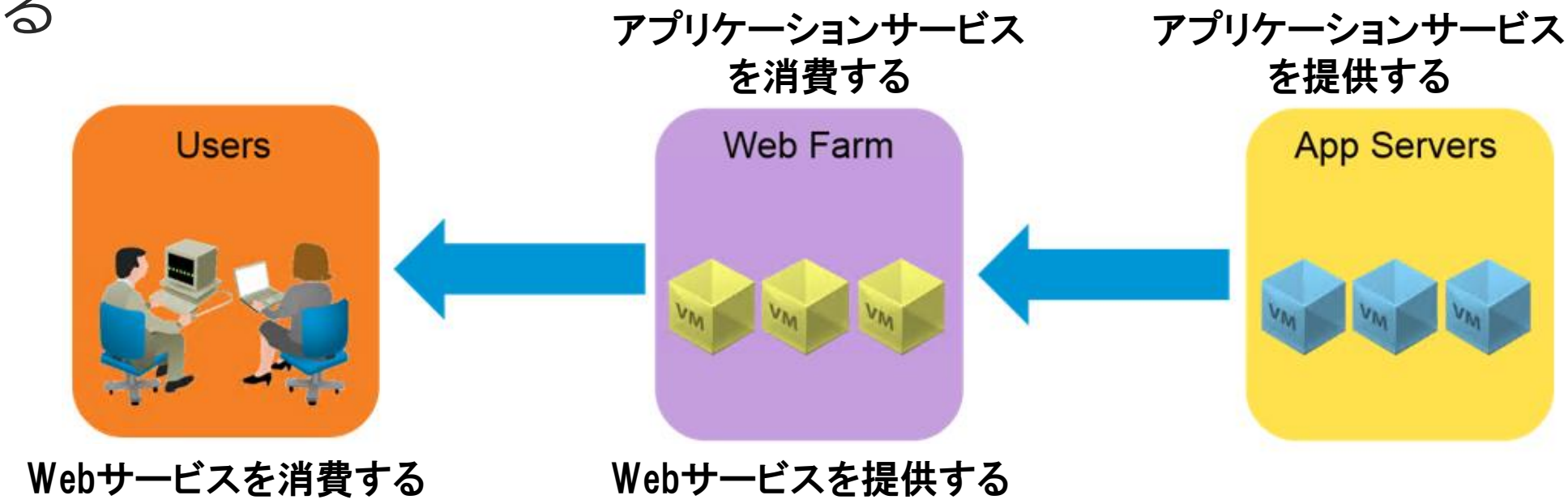
アプリケーション間の通信

- EPGが異なる場合、必ずContractを定義する
- ContractはどのEPGとどのEPGが、どういうルールで通信してよいのかを定義する
- Contractが無いEPG間は通信できない（ホワイトリスト方式）
- EPG間の通信は片方向（monolog）、または両方向（dialog）として定義する

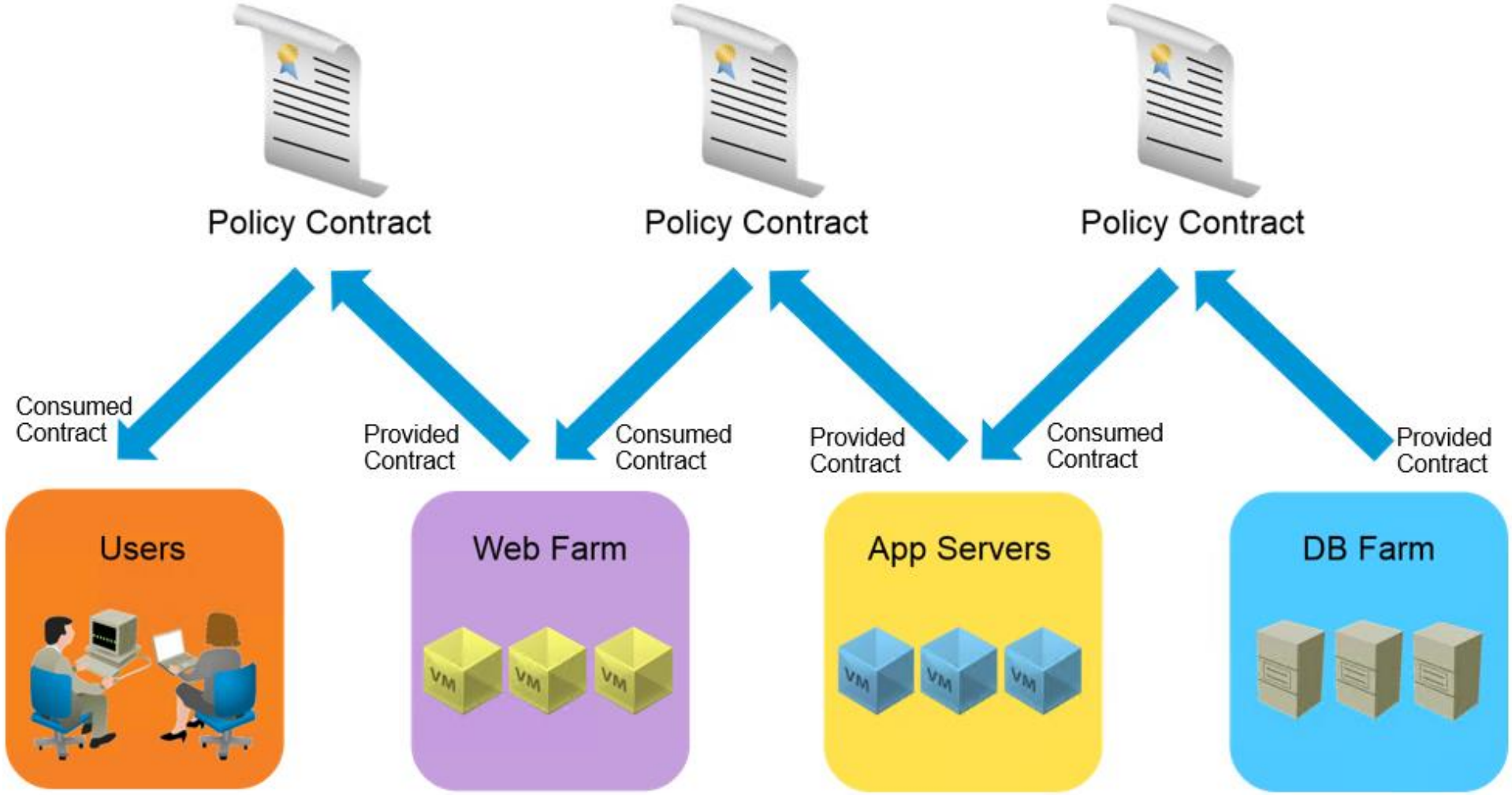


Provider（提供者）とConsumer（消費者）

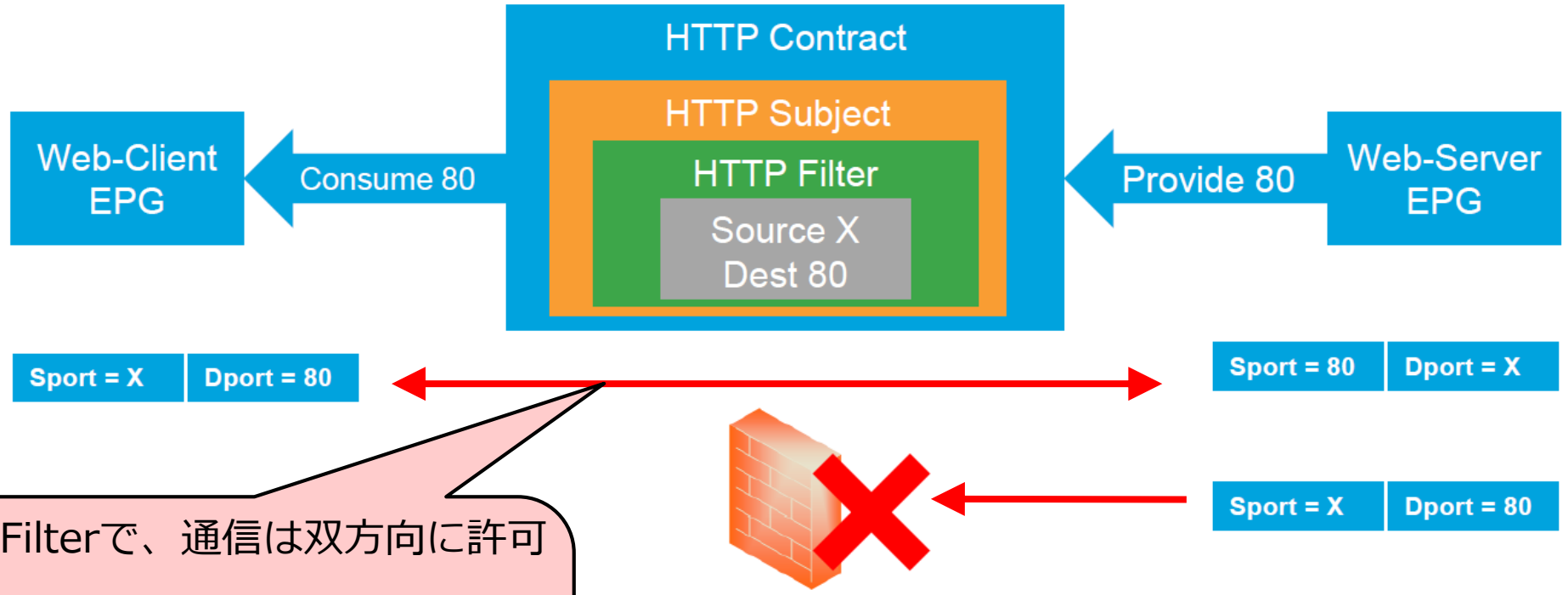
- Provider（提供者）とConsumer（消費者）は、アプリケーション視点で見た接続性の定義
- すべてのオブジェクトは提供者側、消費者側、あるいは両方に対応できる



Provided ContractとConsumed Contract



Contract, Subject, Filter

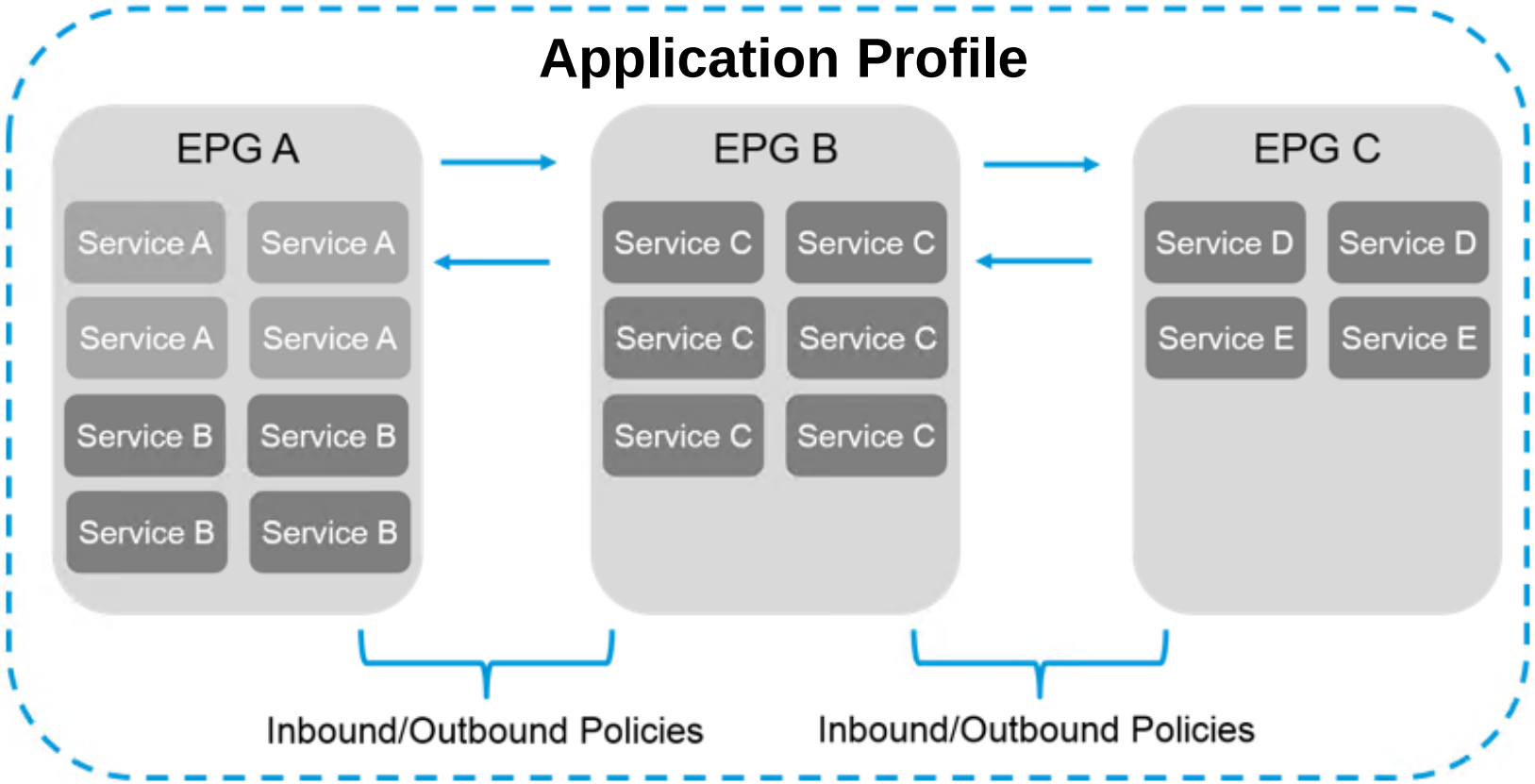


ひとつのFilterで、通信は双方向に許可される

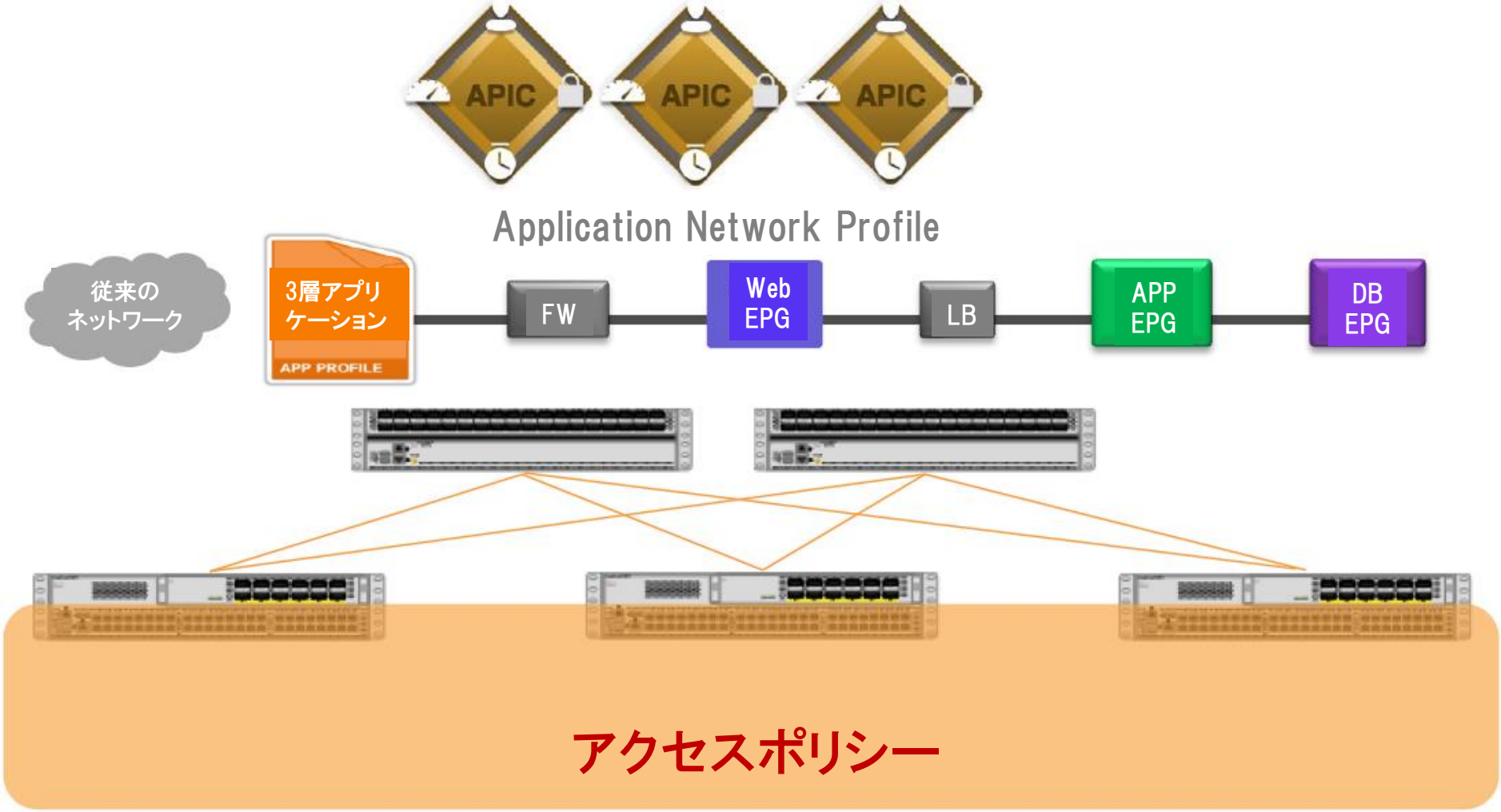
Filterで指定するポートはInitiate側から出力されるパケットで設定する

Application Profile

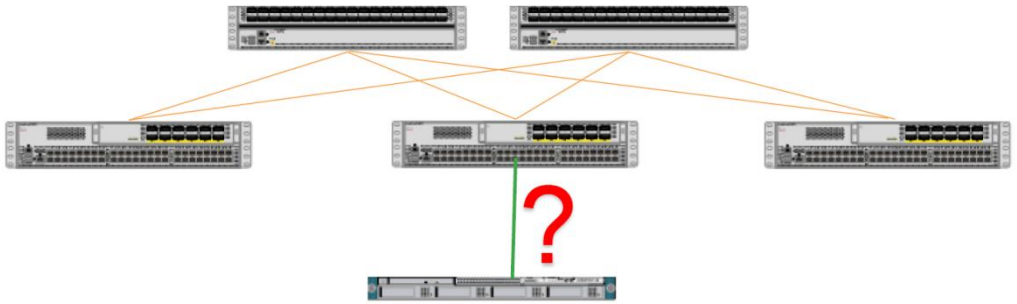
- ひとつのアプリケーションサービスが成立するための定義で、EPGの定義とEPG間の通信ルールであるContract（ポリシー）をまとめたもの



アクセスポリシー

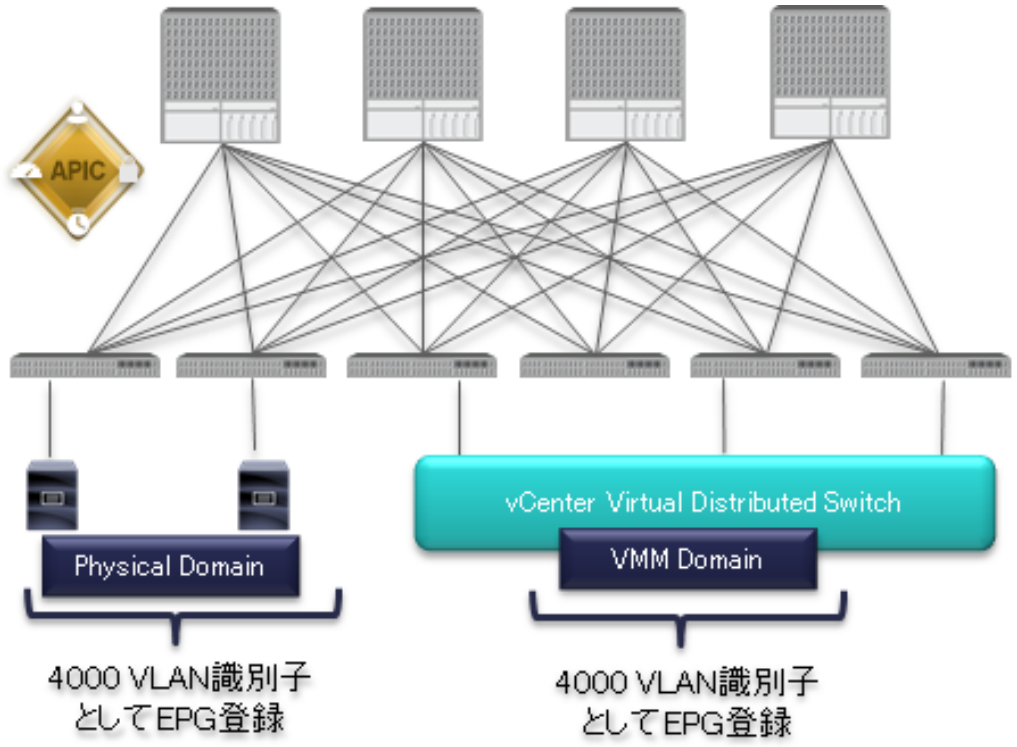


アクセスポリシーの概要



- 従来でいうL1-L2の設定
- 物理ネットワークの設定が含まれる
- Cisco ACIではスイッチポートのリンク速度、STP、CDP、LLDPやチャネル、VLANなどの設定項目を抽象化し、ポリシーとして定義する
- ポリシーをまとめたファブリック・プロファイルを作り、ACIファブリックに対して適用することで、設定を反映
- 作成済みポリシーは再利用可能。別のLeafスイッチやポートに対して同じ設定を迅速に行うことができる
- Switch Profile, Interface Profile, Interface Policy Group, VLAN Pool, Domain, AEPがある

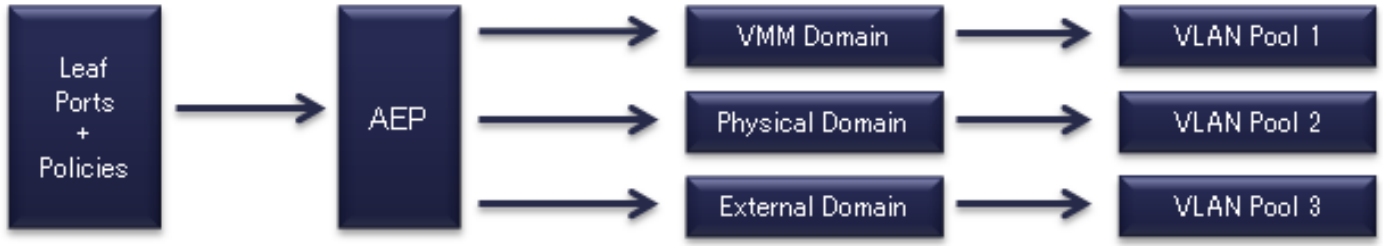
Leaf アクセスポートとドメインの定義



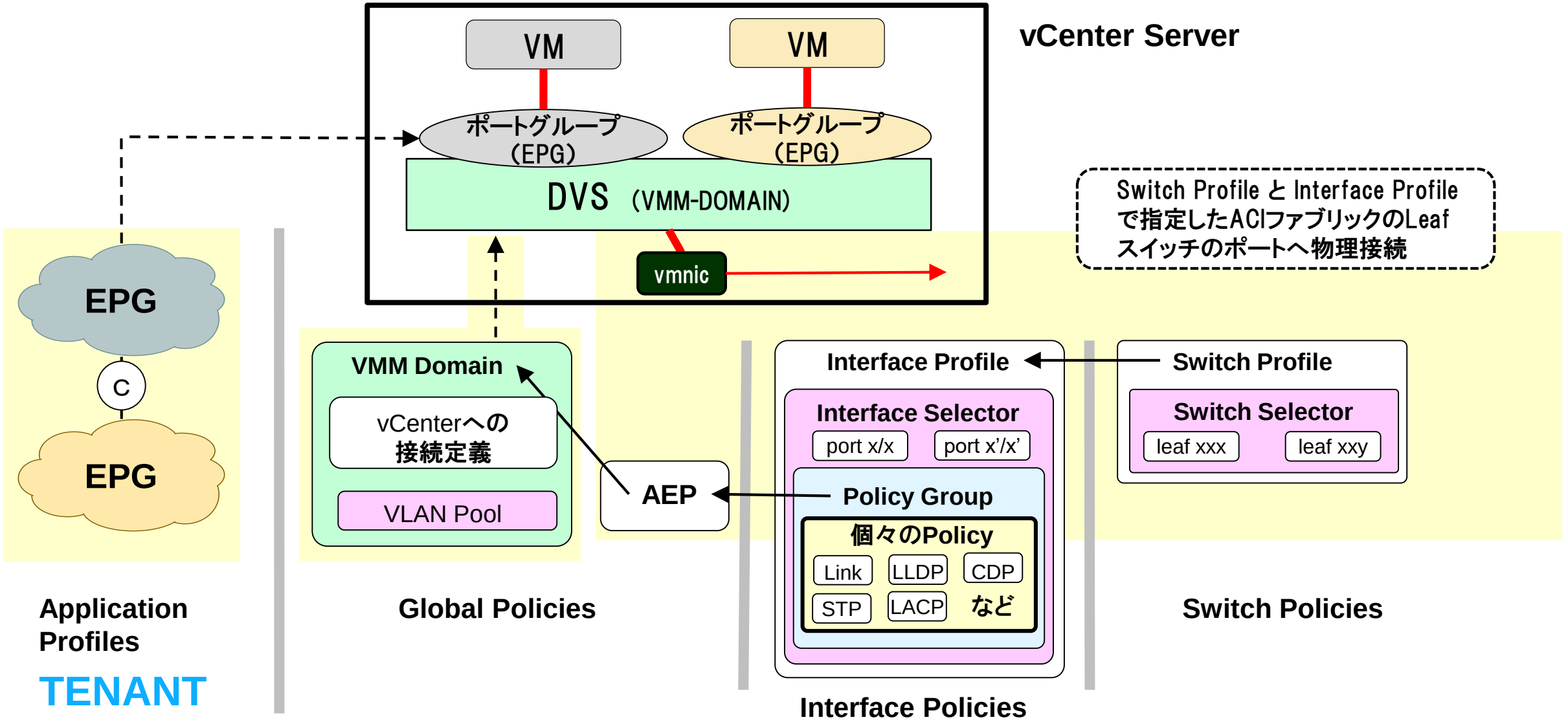
ドメインの種類

VMM Domain ..... Hypervisorへの接続
Physical Domain ..... ベアメタルサーバへの接続
External Domain ..... 外部ネットワークへの接続
L2ネットワーク
L3ネットワーク

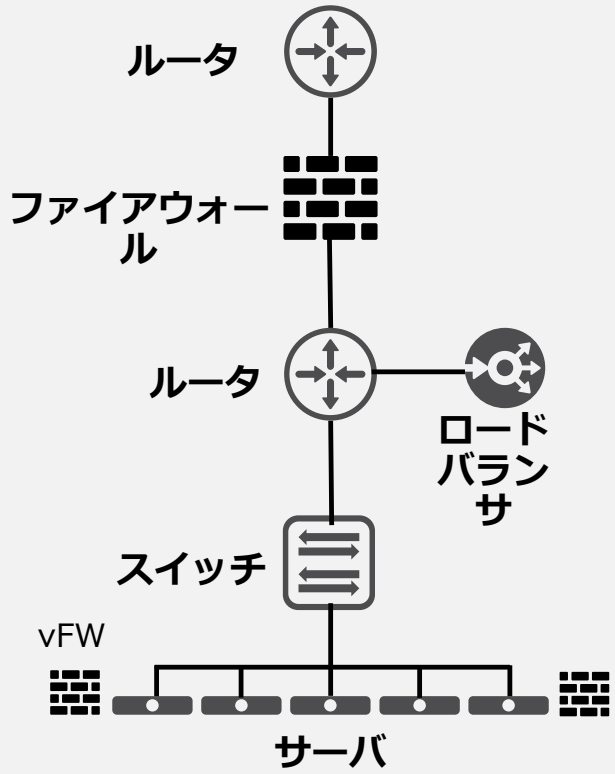
- VLAN Poolの定義
- 各種ドメインの定義
- Interface Policyの作成 ..... インターフェイスのパラメータ定義
- Attachable AEP (Access Entity Profile)の作成 ..... 接続するドメインの定義



参考：VMware VMMドメインを使った接続設定の全体像



従来のネットワークにおけるサービスの挿入



従来型のネットワークにおけるサービスの挿入

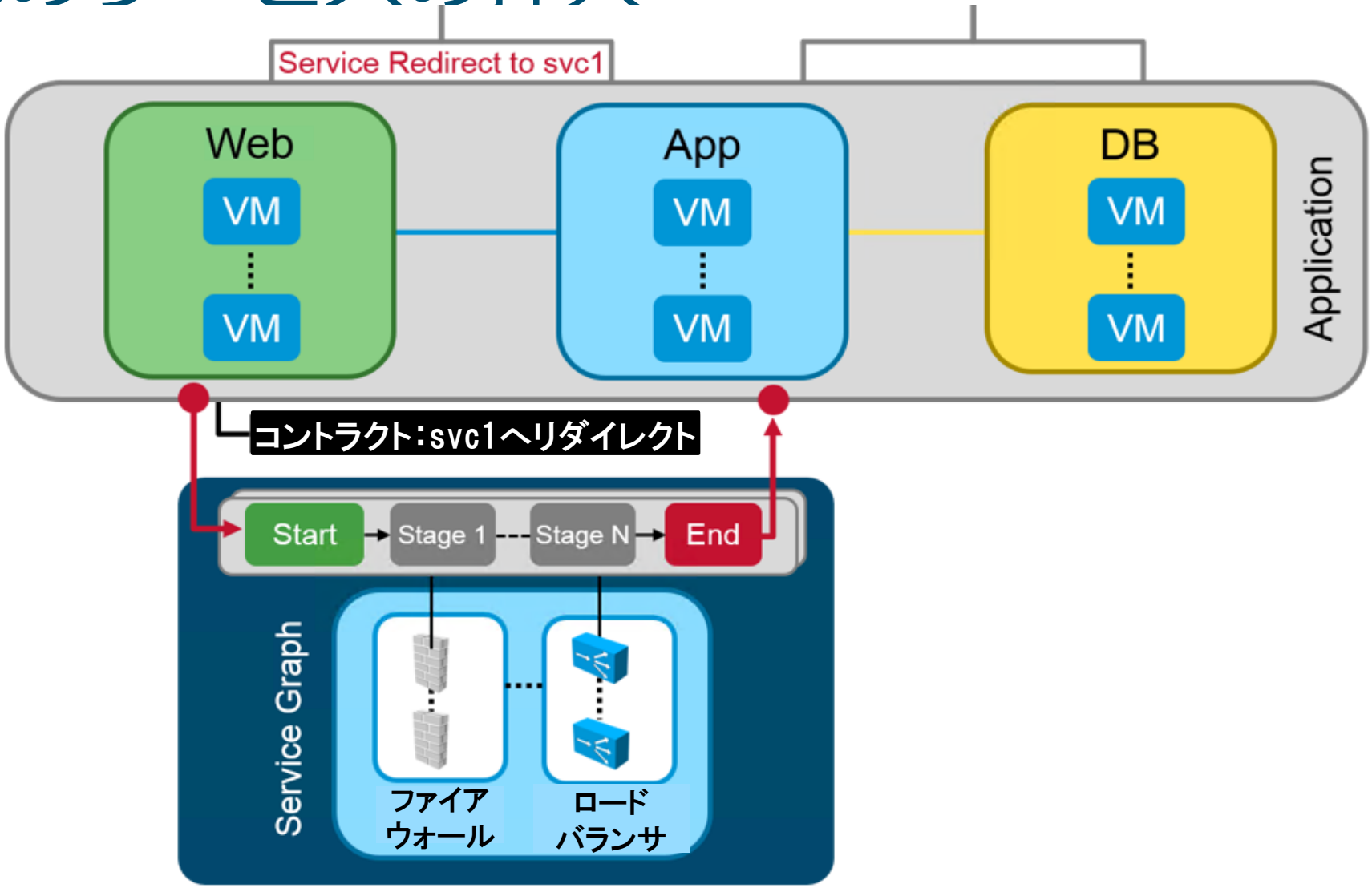
- ファイヤウォールを挿入すべくネットワークを設定
- ファイヤウォールにネットワークパラメータを設定
- アプリケーションの要件をファイアウォールのルールとして設定
- ロードバランサのネットワークパラメータを設定
- ロードバランサを接続しているルータで、トラフィックの迂回を設定
- アプリケーションの要件をロードバランサに設定

サービスの挿入作業は数日がかり

ネットワークのコンフィグには時間がかかり、エラーも起こりやすい

サービスに関する設定をトラッキングするのが難しい

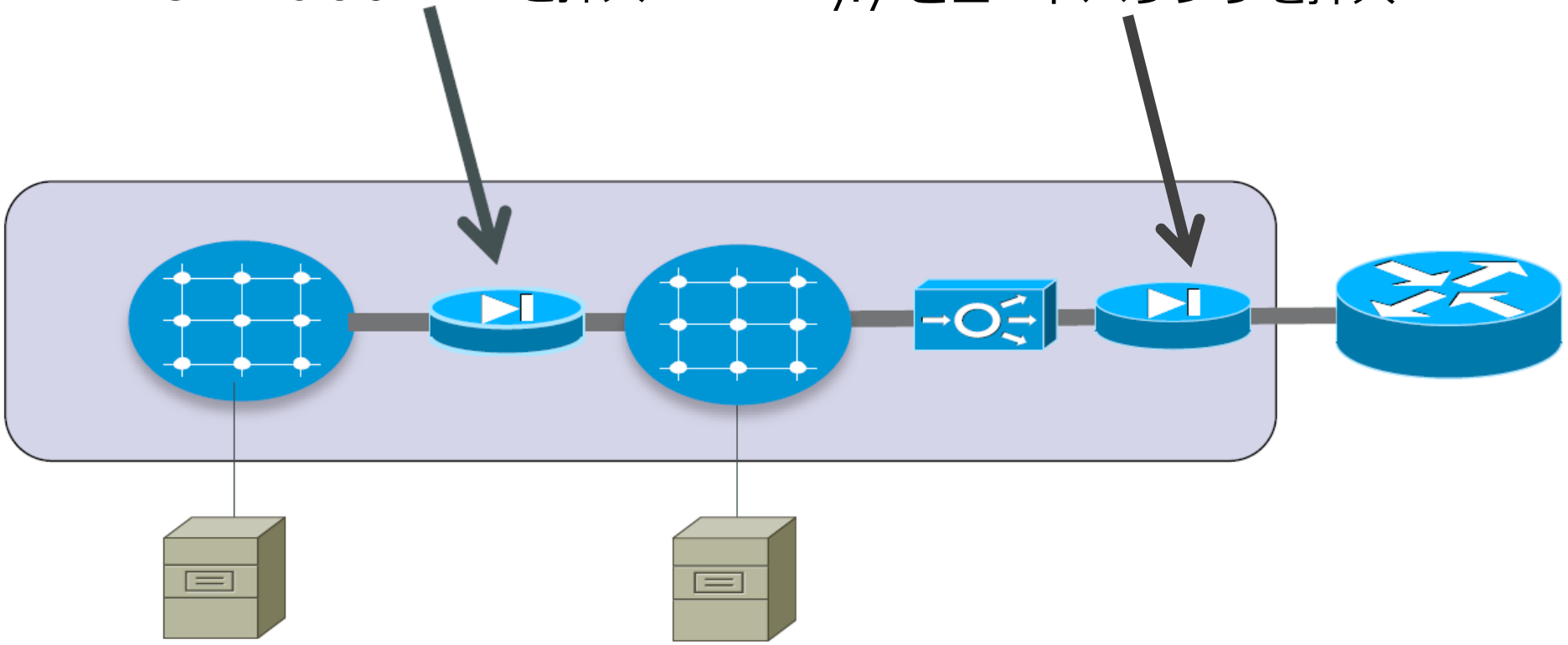
ACIへのサービスの挿入



ACIにおけるサービス挿入モデル

物理サーバと仮想サーバ間に
ASAv version x.x を挿入

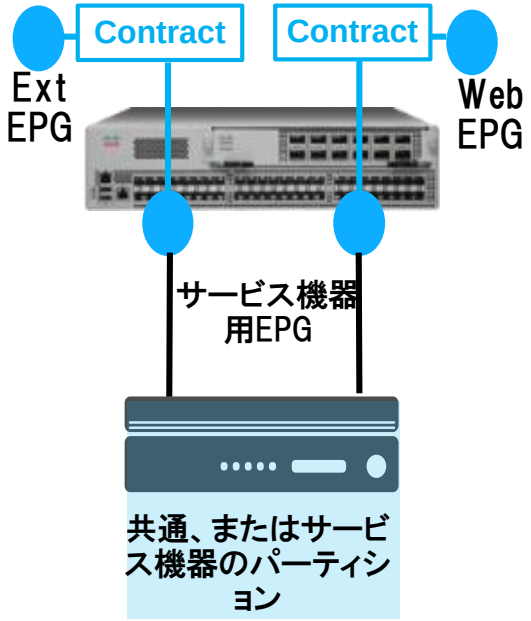
利用者と仮想サーバ間にASAv version
y.y とロードバランサを挿入



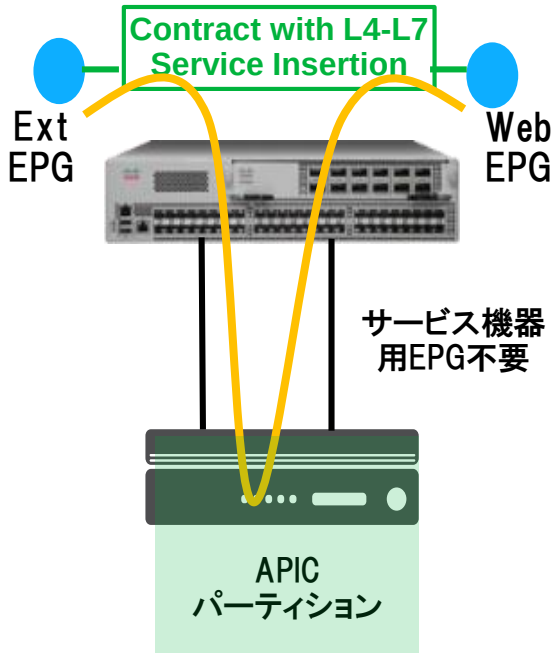
物理サーバ

仮想サーバ

サービス機器の統合モデル

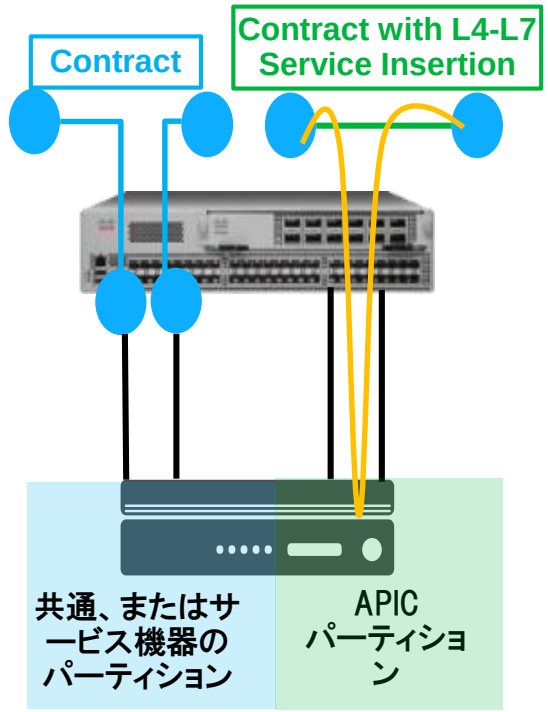


EPGを使った挿入
Service Graphによる
サービスの挿入なし



Service Graphを使って
L4-L7 サービスとして
Cisco ACI に統合

managedモード
Unmanagedモード



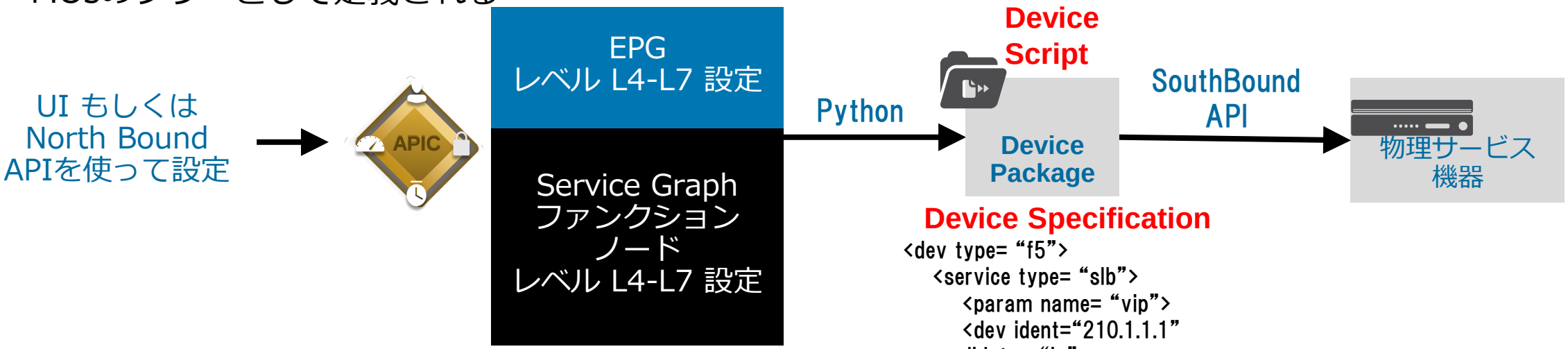
Mix Mode:
L4-L7 サービス挿入のある/なしを混合した統合

managedモードにおけるデバイス定義とDevice Package

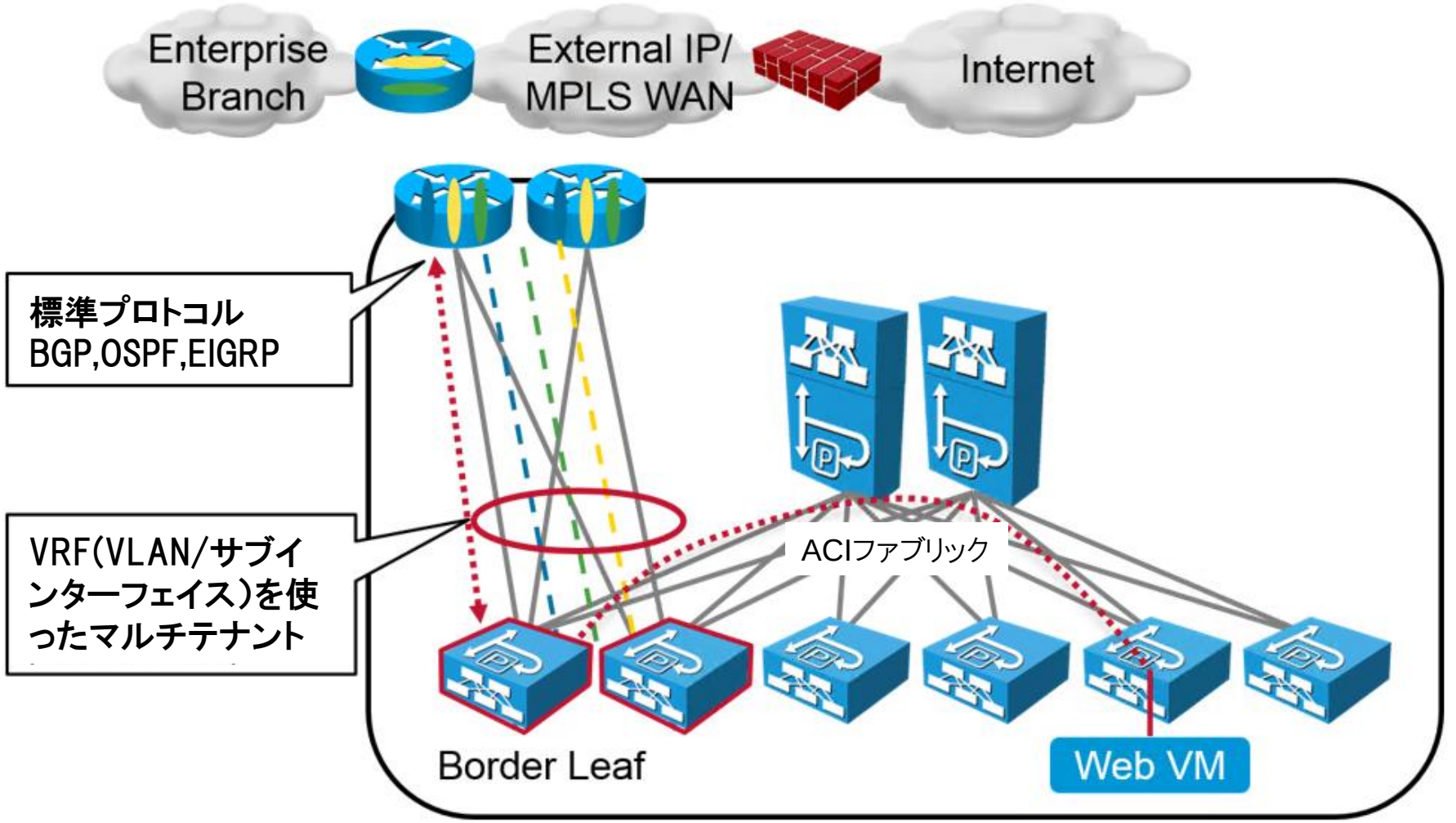
APIC がサービスデバイスと通信するには Device Package が必要
Device Package はZIPファイルで次の2つが含まれている

Device Specification (xml): APICの設定は多数の管理対象オブジェクト（MOs）から成るオブジェクトモデルとして表現される。デバイスタイプは、ルートでのメタデバイス（MDev）を持つMOsのツリーとして定義される

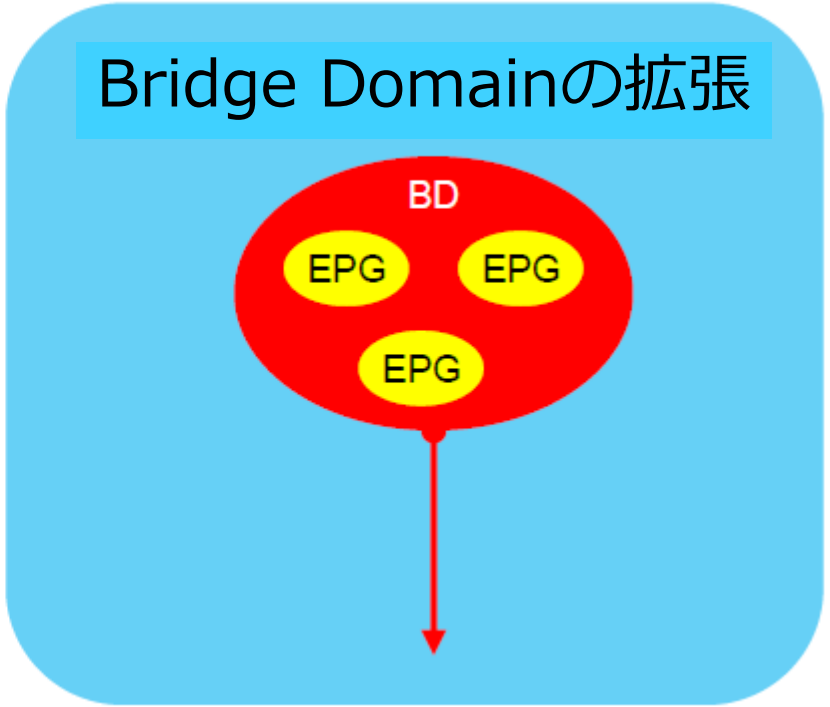
DeviceScript (python): APICとデバイス間統合は、内部定義された APIC イベントファンクションコースをマップするDevice Scriptによる実行される



外部L3ネットワークとの接続

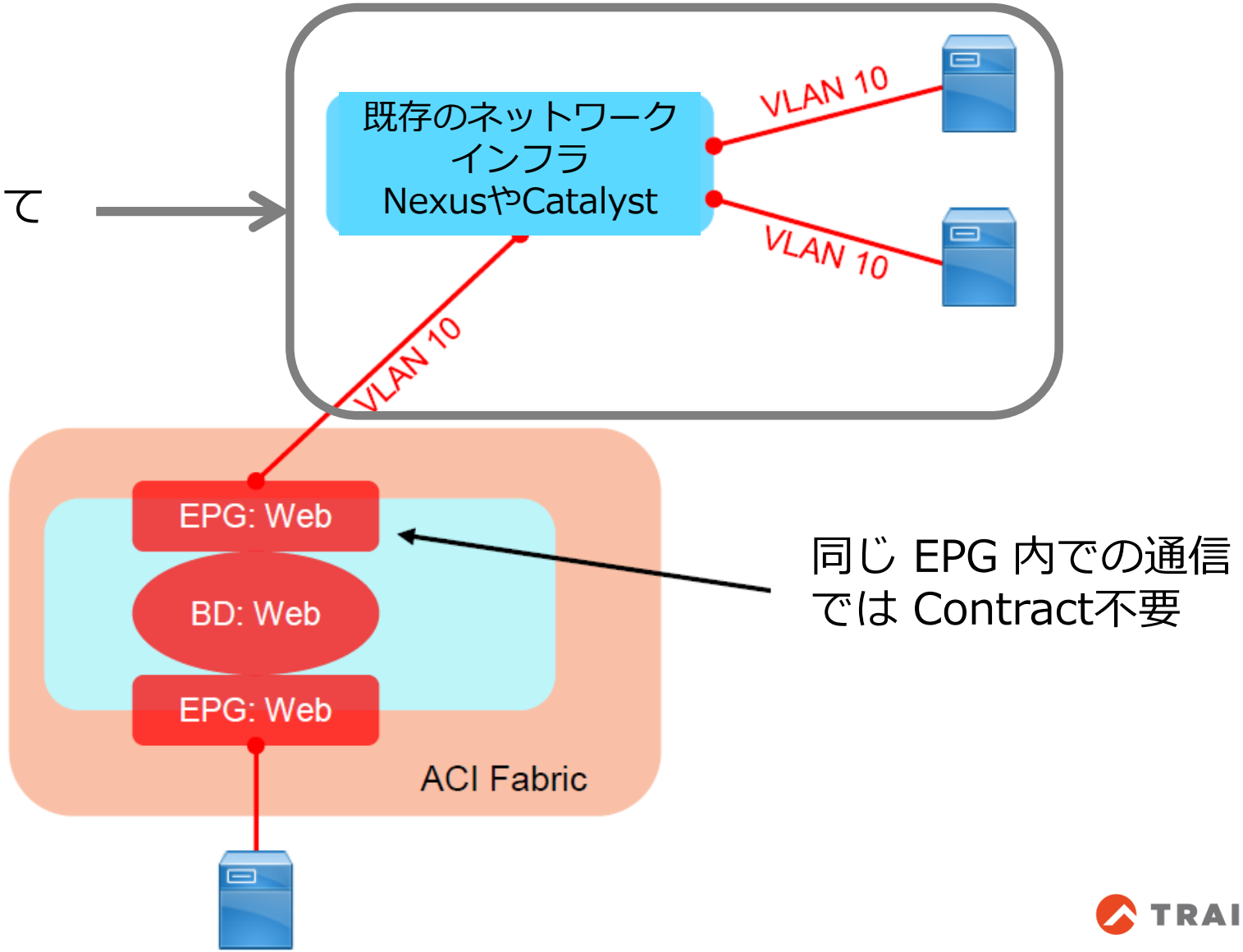


外部L2接続形式



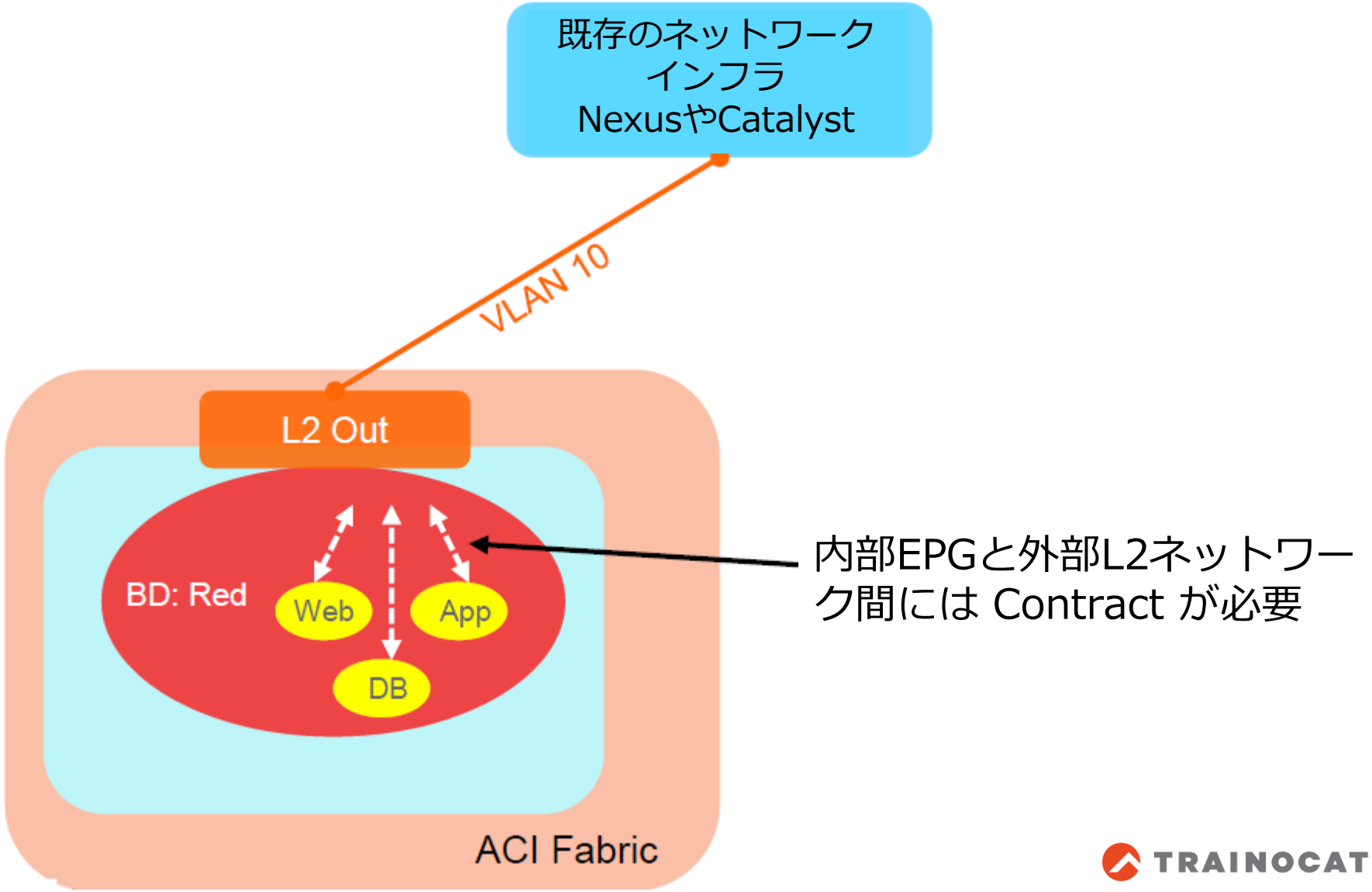
EPGの拡張

VLAN 10を EPG ‘Web’ の一部として扱う



同じ EPG 内での通信では Contract不要

L2 Outsideを使ったBridge Domainの拡張



まとめ

1. Cisco ACIの特徴

- Cisco ACIのDeployモデル
- Cisco ACIファブリックの基本構成
- APICの役割
- Cisco ACIファブリックの統合オーバーレイ
- 正規化

2. ACIのポリシーモデル

- ACIのポリシー
- テナントとコンテキスト
- Bridge DomainとEPG
- コントラクトとApplication Profile
- アクセスポリシー
- ACIへのサービス挿入
- 外部ネットワークとの接続

Thank you

Q & A

画面右側の Q&A ウィンドウから All Panelist 宛に送信してください。

次回の Webcast

[タイトル]
Nexus 9000 シリーズスイッチの
アーキテクチャ概要と基本的なトラブルシューティング

[日程]
2018 年 7 月 10 日 (火) 10:00-11:30

[スピーカー]
山本 大輔 (Daisuke Yamamoto)
シスコ テクニカル サービス, カスタマー サポート エンジニア

※詳細はサポートコミュニティトップページに掲載中です。

ご参加ありがとうございました。

アンケートにもぜひご協力ください。


CISCO