Pluribus NETWORKS

マクロセグメンテーションで よりセキュアなIT環境を

マーコ・ペッシー Marco Pessi
Sr. Technical Product Manager
Pluribus Networks

1/27/2017
Dell Seminar@ITMedia

トピック

- ファブリックをセキュアにするには
  - ファブリック管理
  - マルチテナント (プライベート仮想ネットワーク) の使用
  - コントロールプレーンをセキュアに
  - セキュリティサービスの挿入
  - ネットワーク分析

  上記をすべて活用した **Fabric Security Architecture**

Virtualization Centric Fabric – VCF

アプリケーションの可視性

Built-in, no taps, no brokers, no expensive tools

マルチテナント
仮想プライベートネットワーク

セキュリティサービスの投入

Granular flow control for conditional security insertion policies

すべてのノードをCLI、API から一元管理

別途コントローラー不要
新しいプロトコルは使用していません
→ *100% interoperable*

Distributed Peer-to-Peer Cluster – Configuration State Consistency (with rollback)

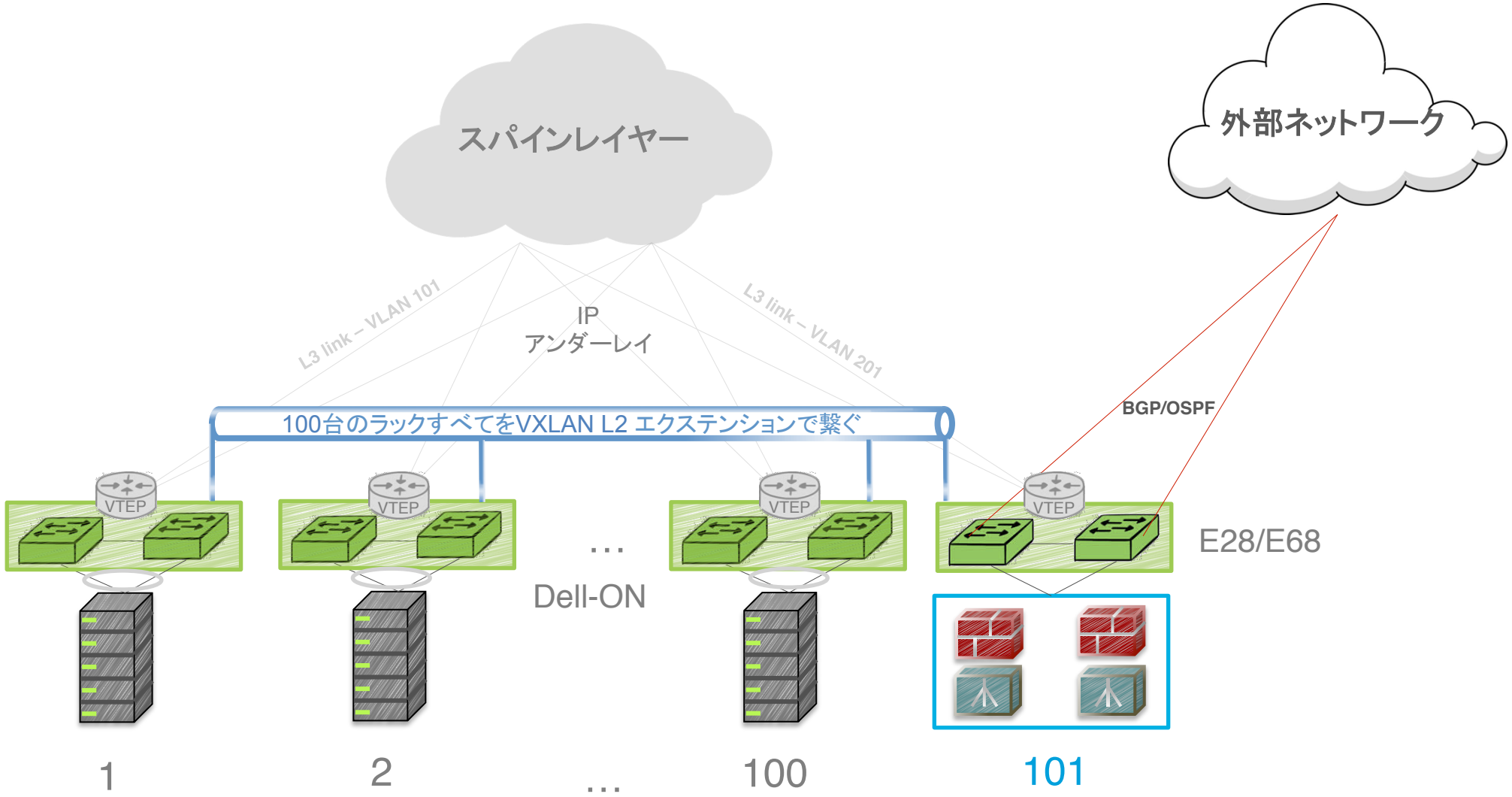
TCP L2/L3/VXLAN Open Networking

TCP L2/L3/VXLAN Open Networking

TCP L2/L3/VXLAN Open Networking

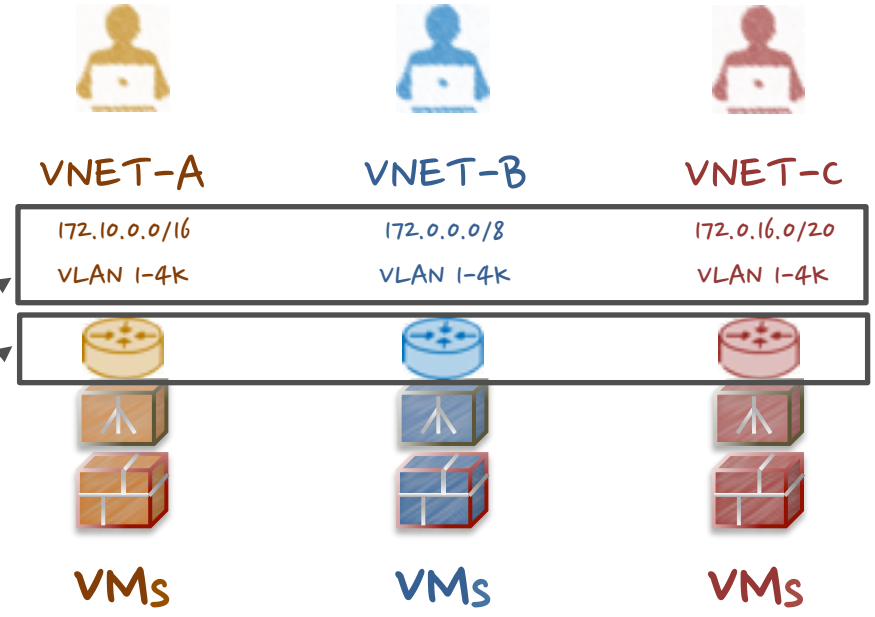
TCP L2/L3/VXLAN Open Networking

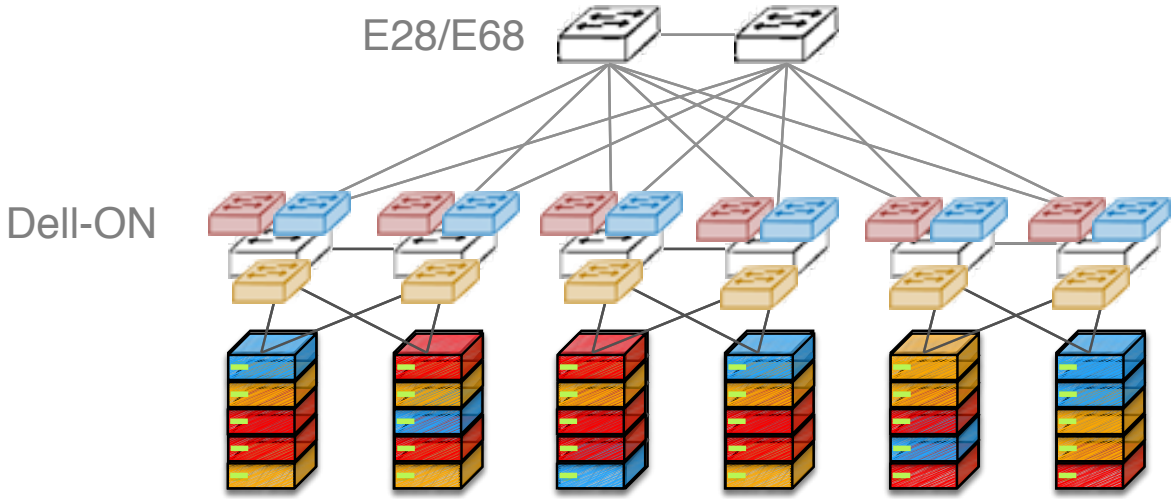
スケールアウトしたファブリックを守るには



プライベート仮想ネットワーク (VNET)
アジャイルなマルチテナント

- **management, control と data plane が隔離された**仮想PODs (vPODs)としての仮想ネットワーク (VNETs)をすばやくプロビジョニング
- 独立したテナントネットワーク
  - 重複したサブネット使用可 (VLANs and IP prefixes)
  - 各VNETに独立した vRouter を作成します
- 独立したマネージメントプレーン
  - プロビジョニング
  - テナントごとにフロー、セービスやVMを可視化します

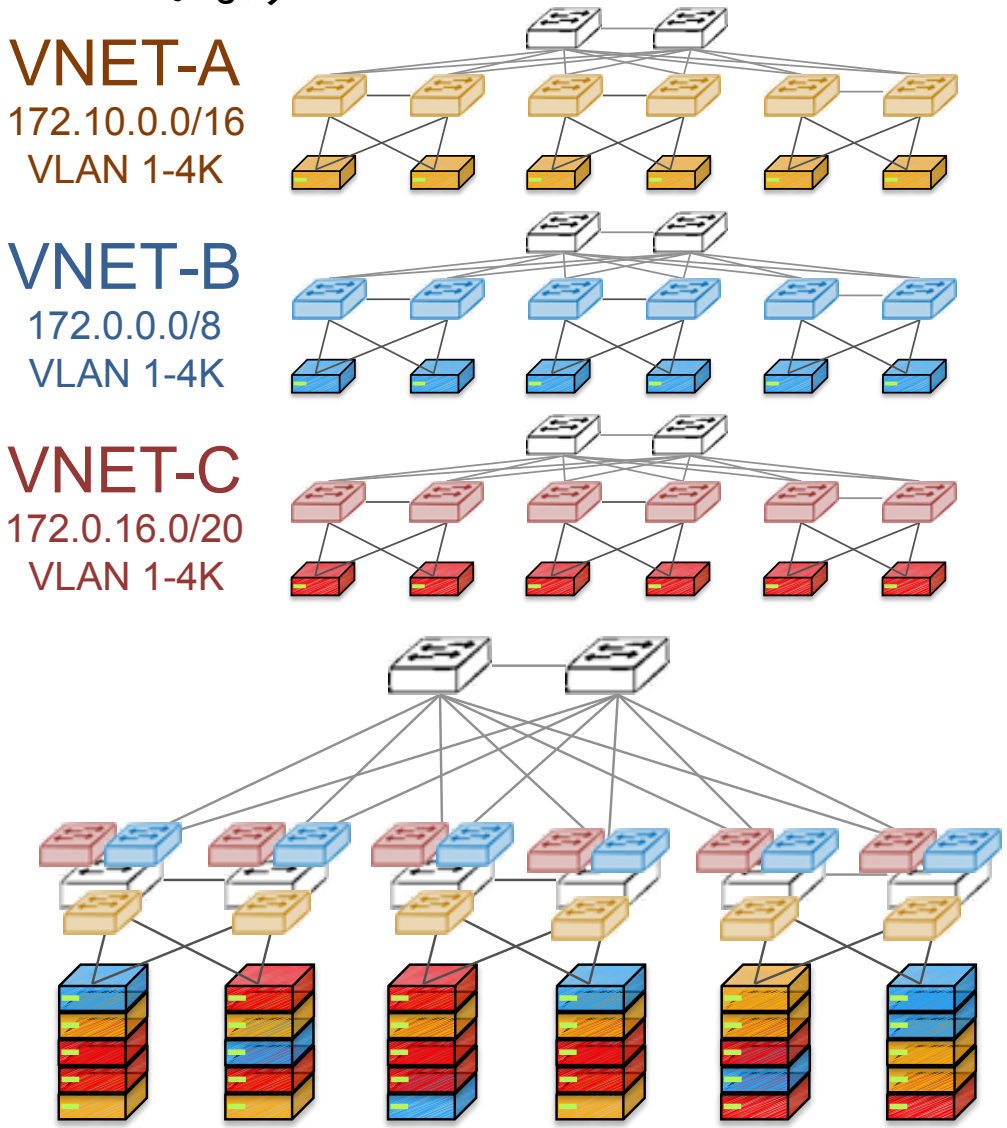




プライベート仮想ネットワーク (VNET)
マルチテナントをセキュアに

*Eシリーズ(E28/E68)のみでサポートされています

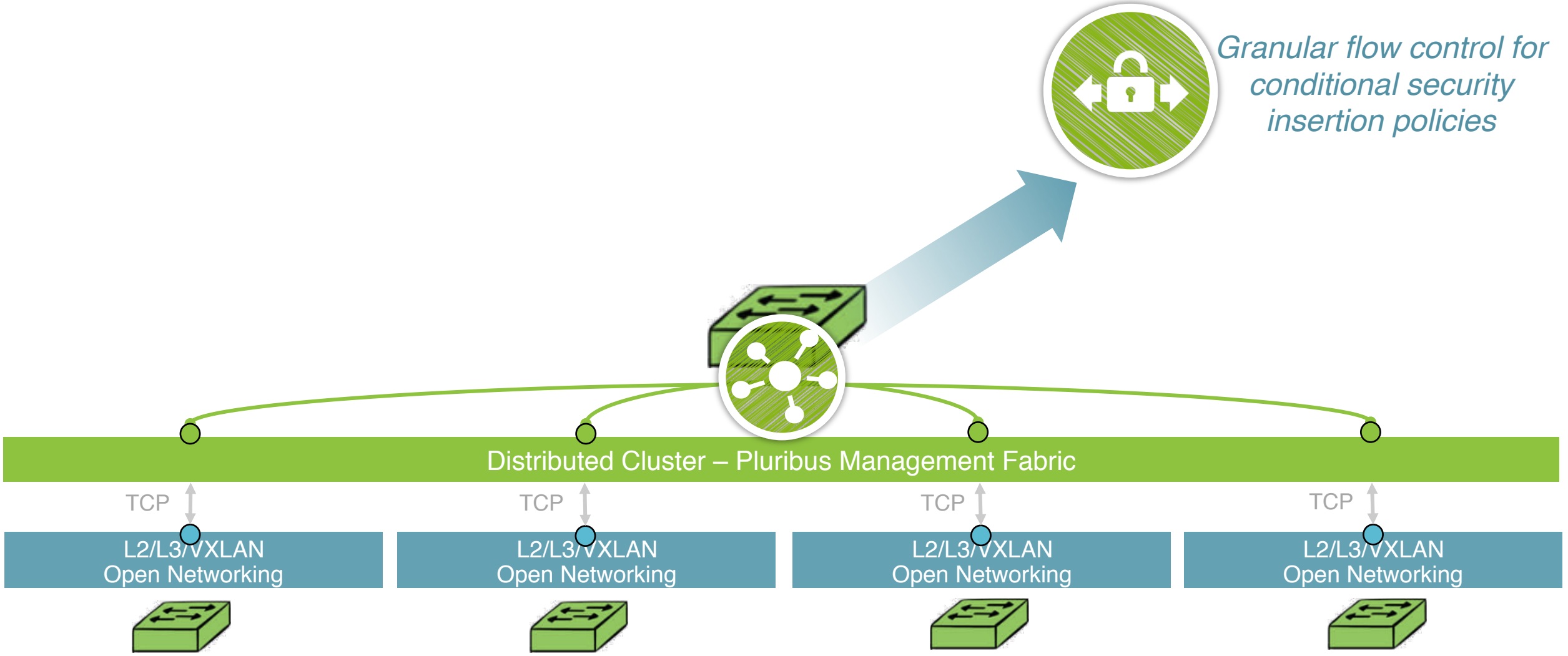
- インフラネットワークにセキュアにアクセス
  - シンプルなテナントネットワークビューを共有トランスポートネットワークから隔離します
- データプレーンの隔離
  - テナント間で漏れを防ぐため自動でVLAN, VRF and VXLAN VNI スペースをオーケストレーションします
  - Anti-spoofing mechanism
- コントロールプレーンの隔離
  - スイッチOS内の専用のコンテナの中でそのテナント用のルーターが走っています。



Virtualization Centric Fabric – VCF

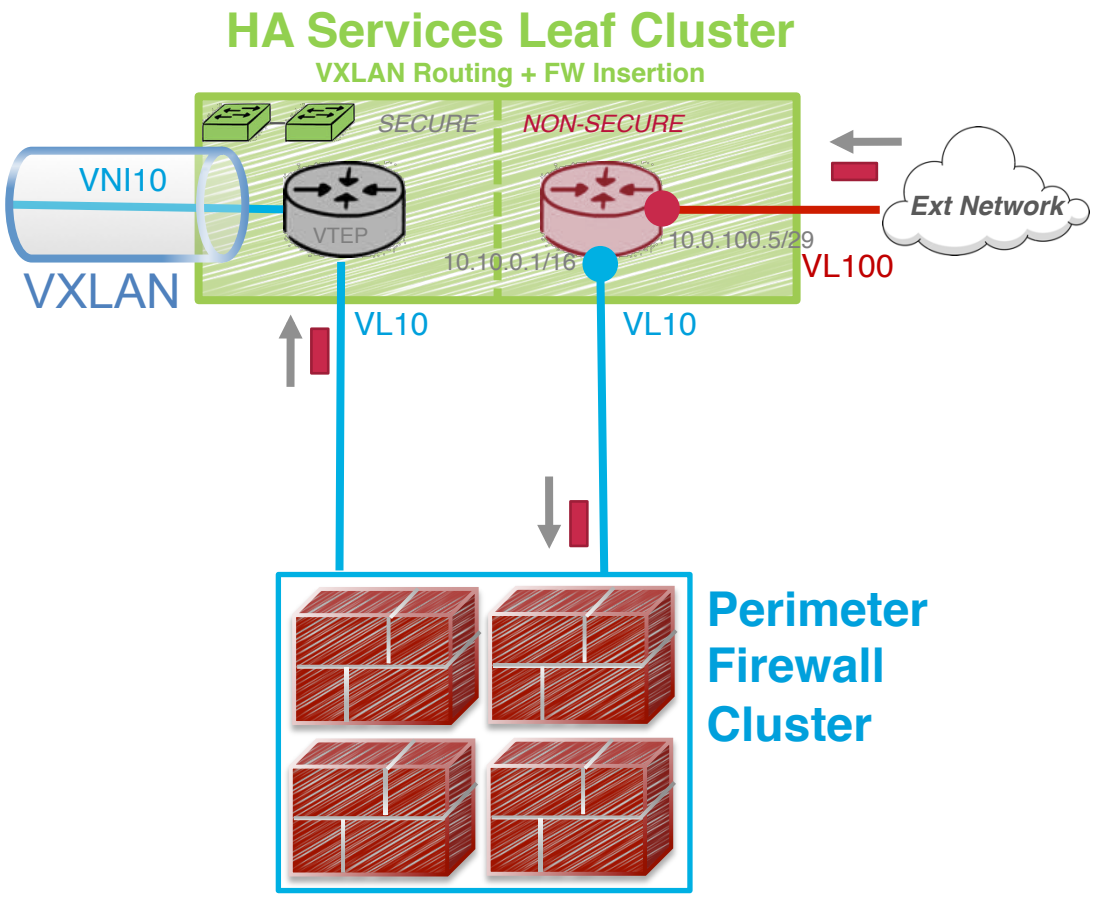
vFlow テクノロジー

セキュリティーサービスの投入



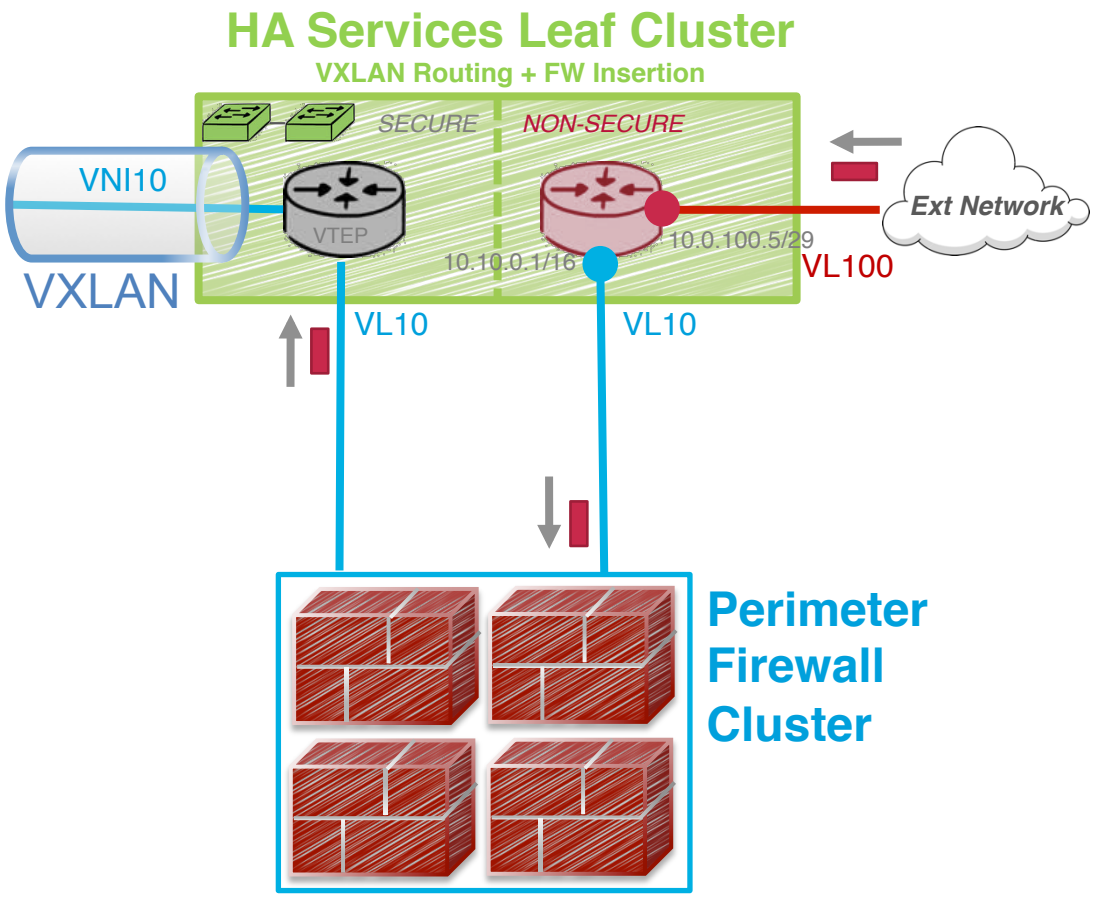
条件つきのセキュリティサービスの挿入
Provide Inspection to untrusted N-S traffic

1. デフォルトトラフィックのためのファイヤーフォールサービス挿入

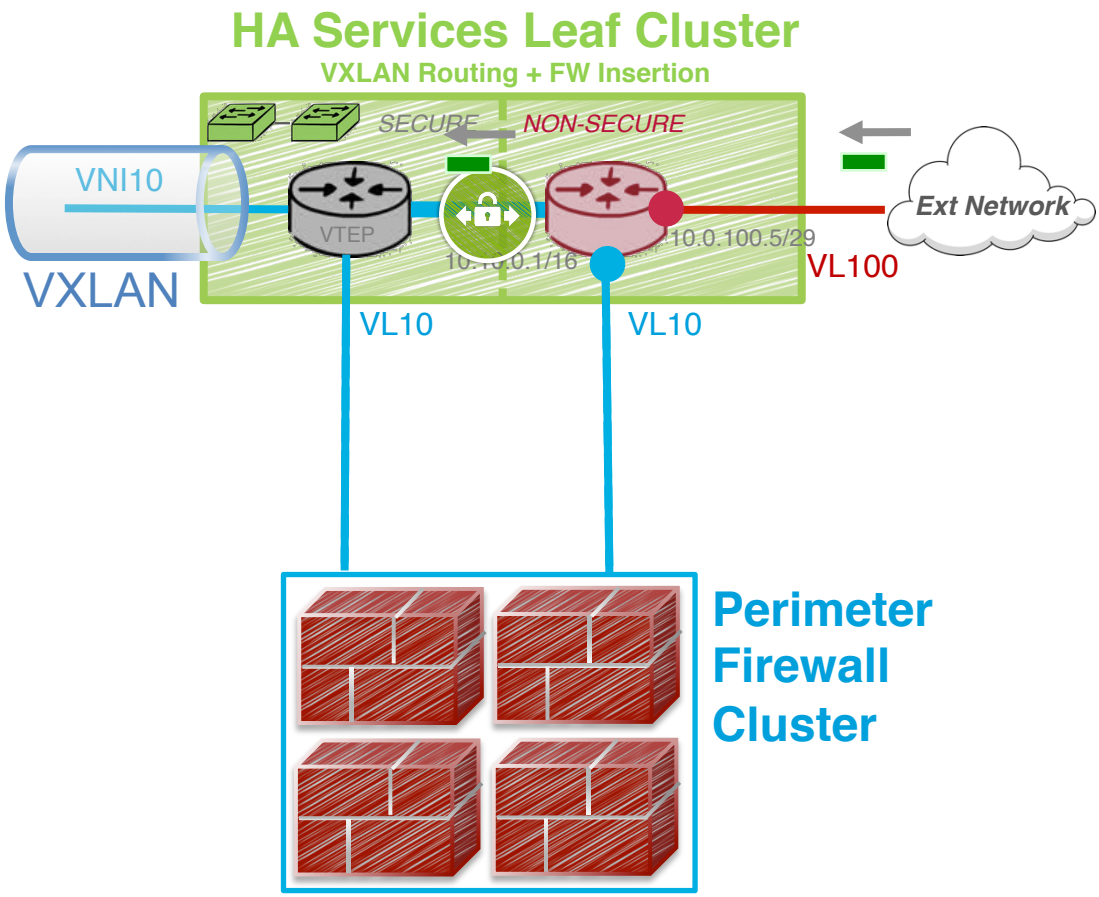


条件付きセキュリティサービスの挿入
Provide Inspection only to untrusted N-S traffic

1. デフォルトトラフィックのためのファイヤーウォールサービスの挿入

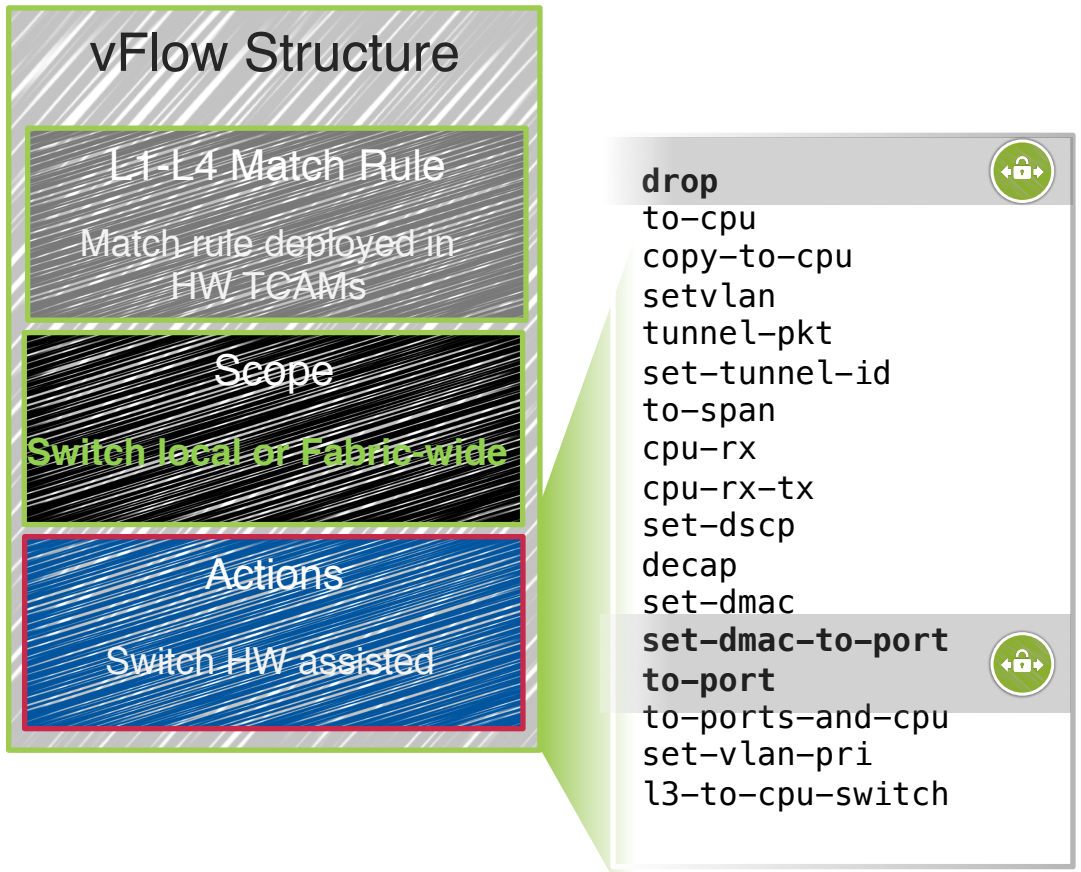


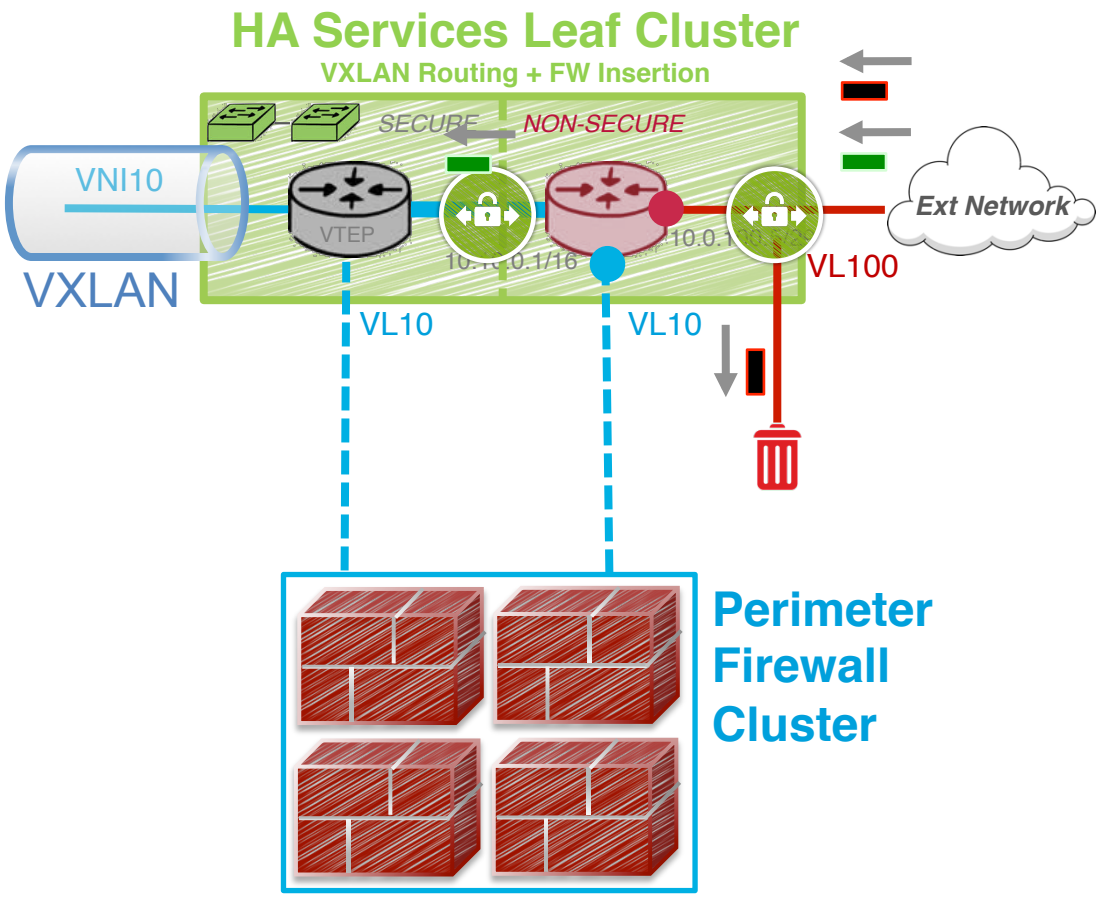
2. セキュアなトラフィックはファイヤーフォールをバイパスします



セキュリティ対策にvFlow でフィルタリングをかける
ラインレートでリダイレクト& ポリシーの執行

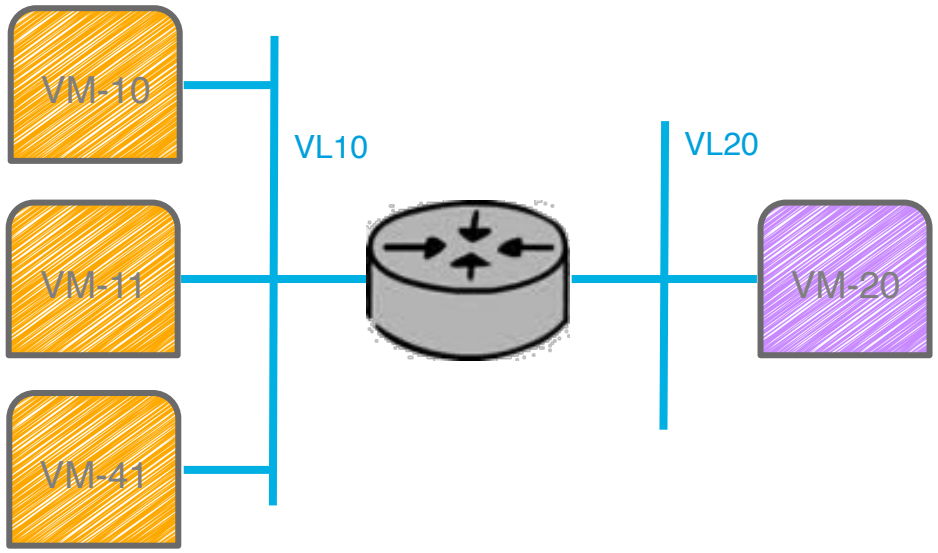
2. セキュアなトラフィックはファイヤーフォールをバイパスします
3. ラインレートでポリシーの執行



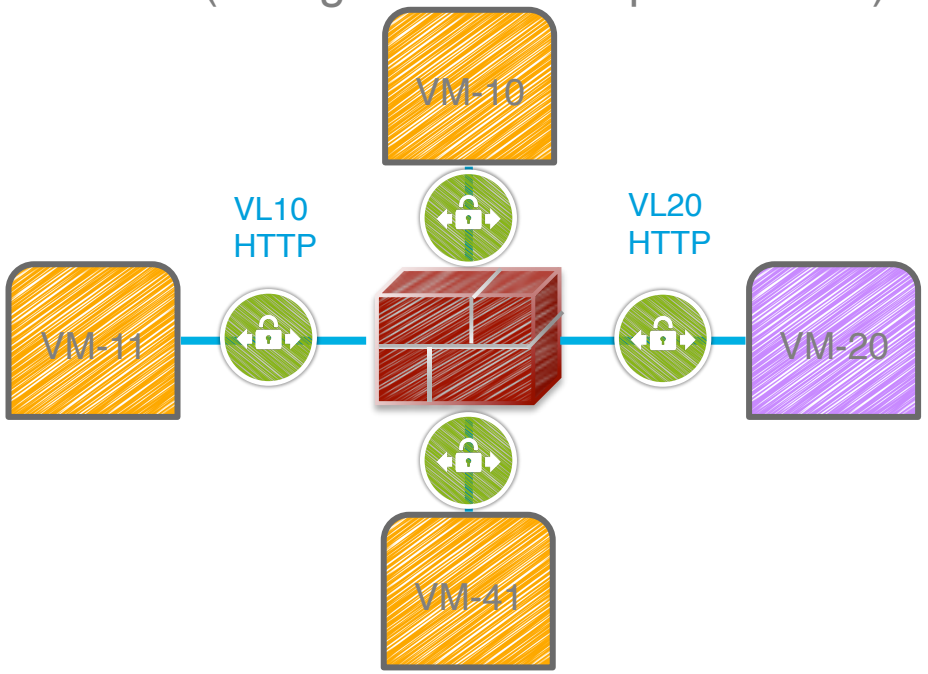


条件付きセキュリティサービスの挿入
Configurable line rate redirection of E-W traffic

1. 通常はこちら: no inspection
   - ファブリックはE-W トラフィックをブリッチしルーティングされます。

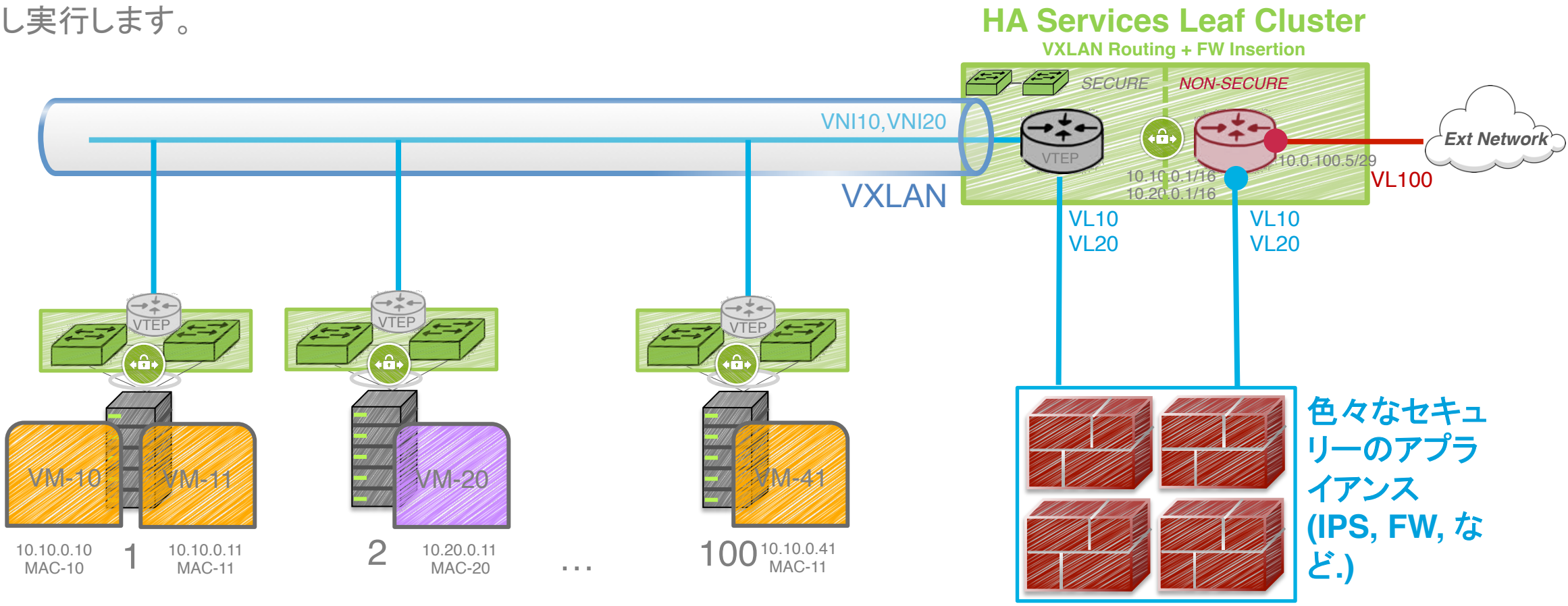


2. 条件つきのセキュリティサービスの挿入
   - ファブリックは選択されたトラフィックをセキュリティアプライアンスへ転送します。(configurable L1-L4 parameters)



E-W & N-S トラフィックに条件に基づいたセキュリティーポリシーを挿入

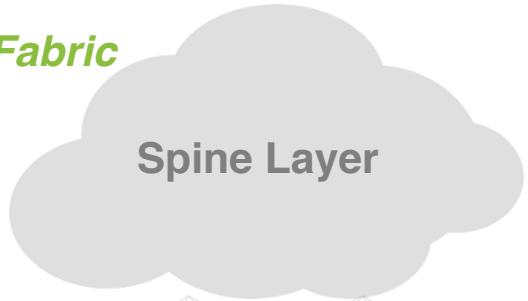
- リーフスイッチは、選択されたセキュリティサービスをブリッチまたはルーチングされた E-W トラフィックに対しファブリックワイドでポリシーを執行し実行します。



すべて合わせて: Fabric Security Architecture

Virtualization Centric Fabric

ポリシーをE-W または N-S トラフィックに対し
ファブリックスコープでプログラミング



- Spine is simple L3 non-blocking interconnect
- Underlay provides inter-rack reachability
- All links are active

L3 link – VLAN 101

IP
underlay

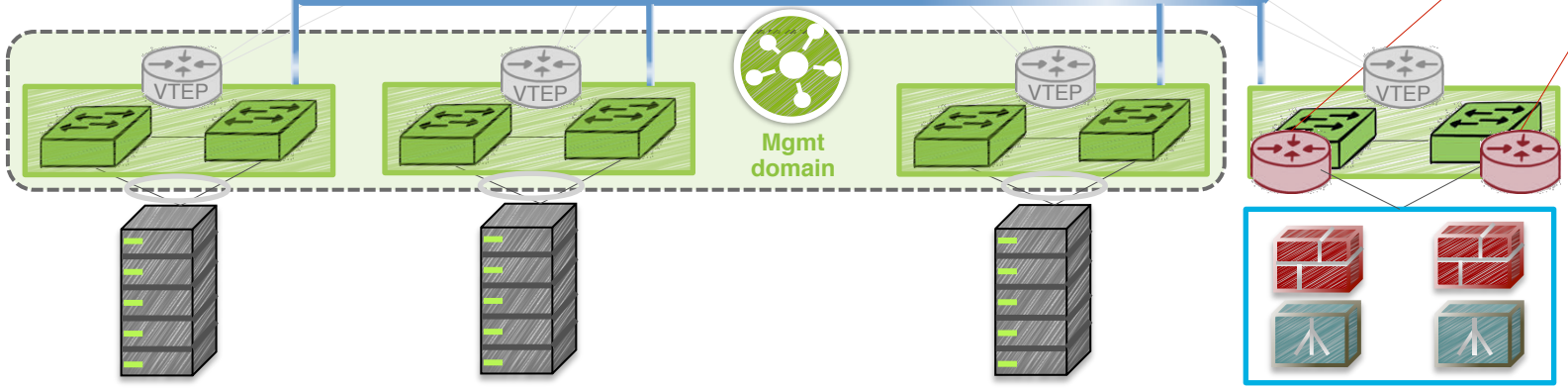
L3 link – VLAN 201

BGP/OSPF

VXLAN L2 Extension Across All 100 Racks

HA Leaf Services

- HA VTEP
- Active-Active LAG towards servers



1 2 … 100 101

Edge Security Services Rack

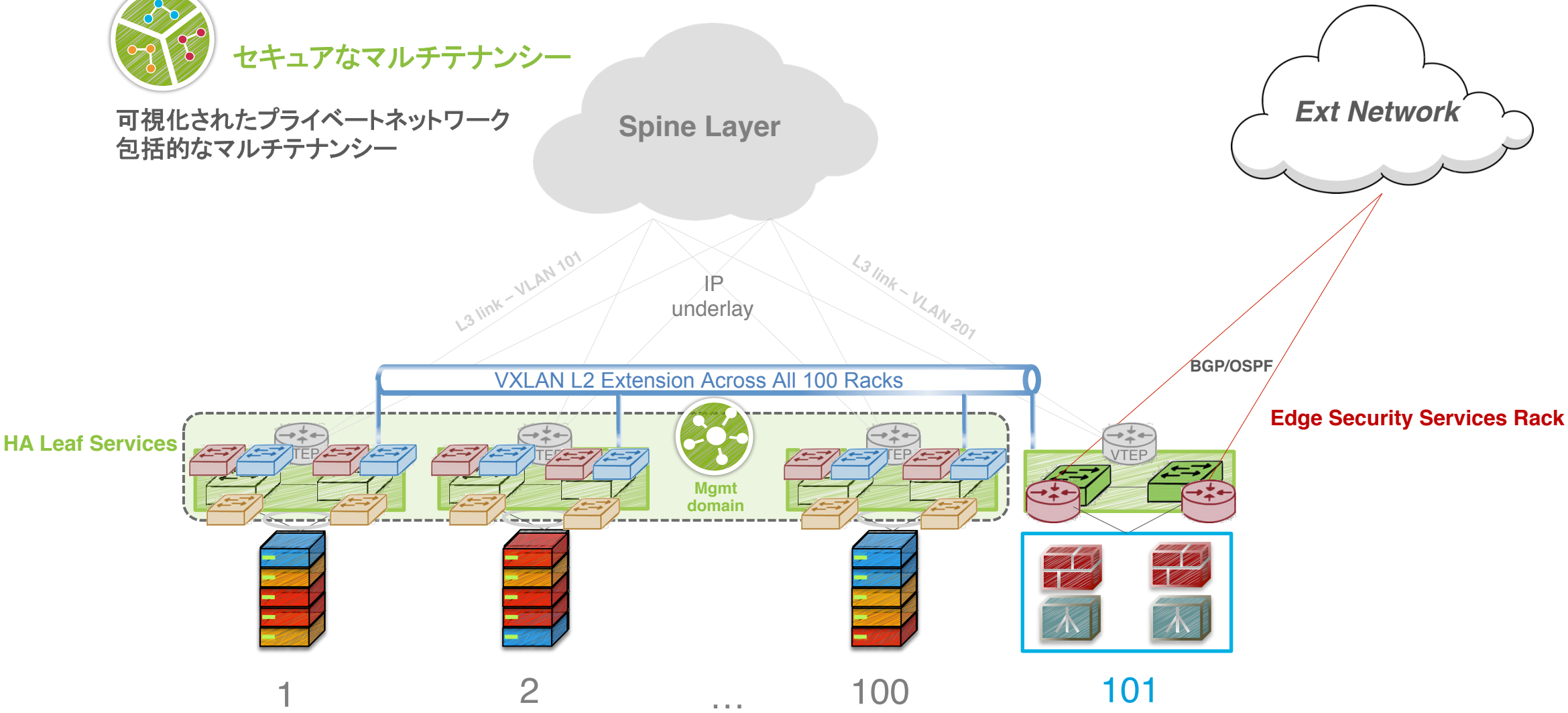
- Grey vRouter for VTEP, Red vRouter to DC network

Pluribus NETWORKS

すべて合わせて: Fabric Security Architecture

セキュアなマルチテナンシー

可視化されたプライベートネットワーク
包括的なマルチテナンシー

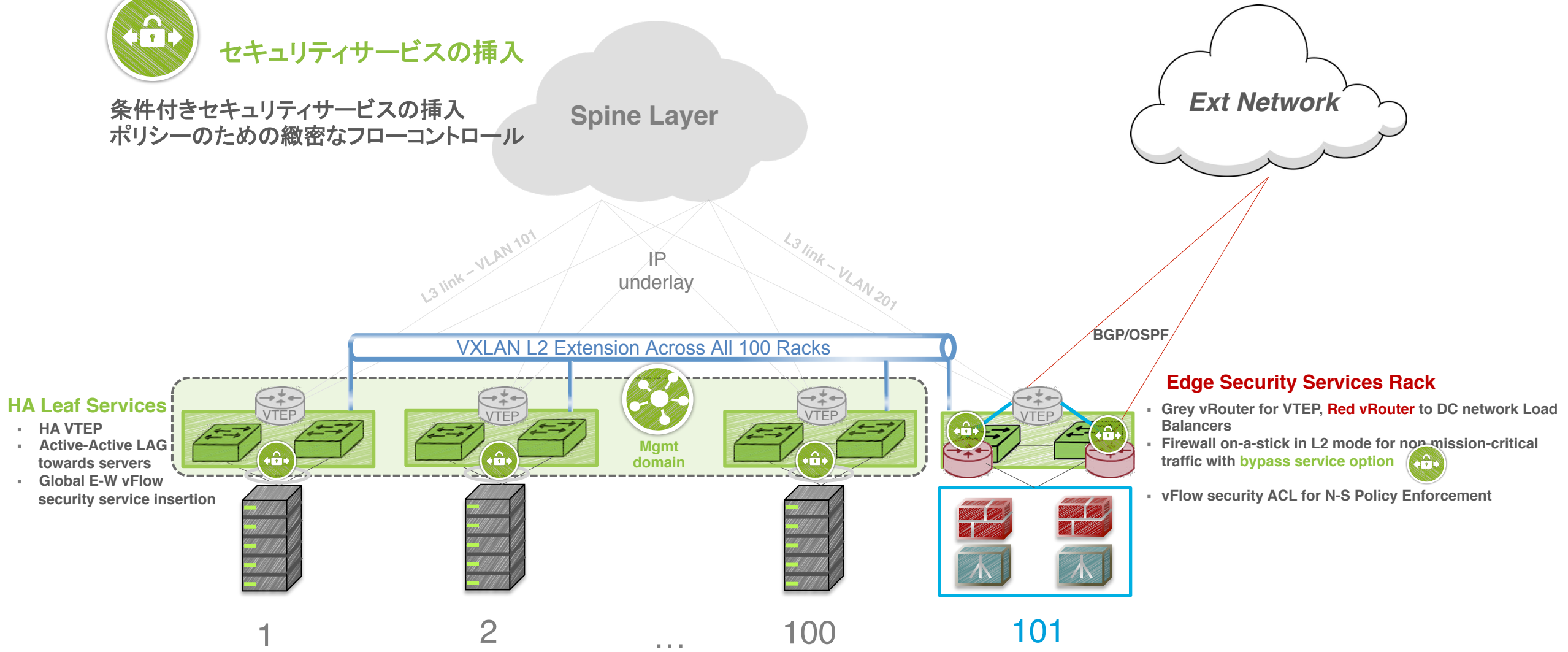


Pluribus NETWORKS

すべて合わせて: Fabric Security Architecture

セキュリティサービスの挿入

条件付きセキュリティサービスの挿入
ポリシーのための緻密なフローコントロール



HA Leaf Services

- HA VTEP
- Active-Active LAG towards servers
- Global E-W vFlow security service insertion

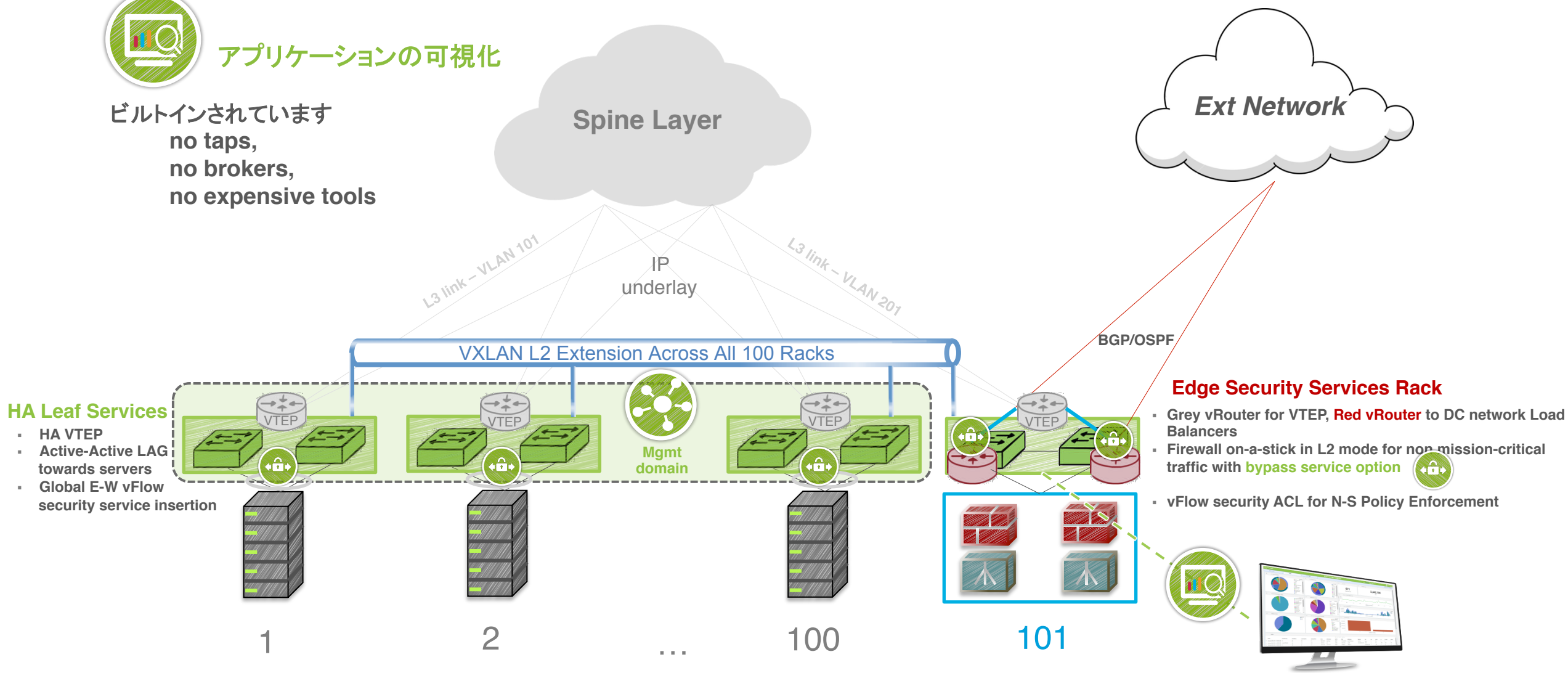
Edge Security Services Rack

- Grey vRouter for VTEP, Red vRouter to DC network Load Balancers
- Firewall on-a-stick in L2 mode for non-mission-critical traffic with bypass service option
- vFlow security ACL for N-S Policy Enforcement

すべて合わせて: Fabric Security Architecture

アプリケーションの可視化

ビルトインされています
no taps,
no brokers,
no expensive tools

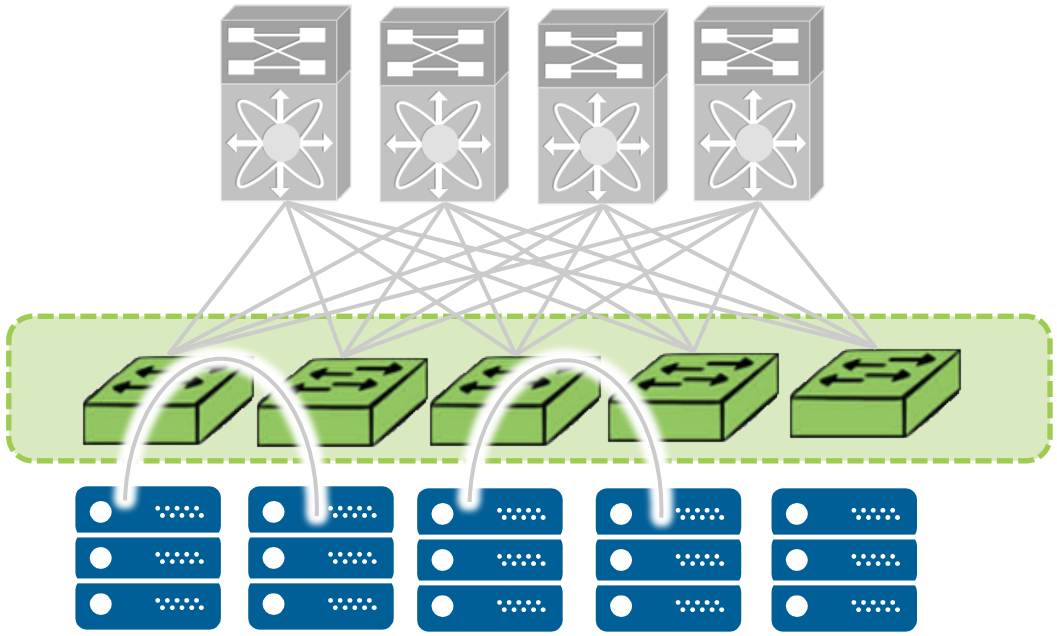


HA Leaf Services
- HA VTEP
- Active-Active LAG towards servers
- Global E-W vFlow security service insertion

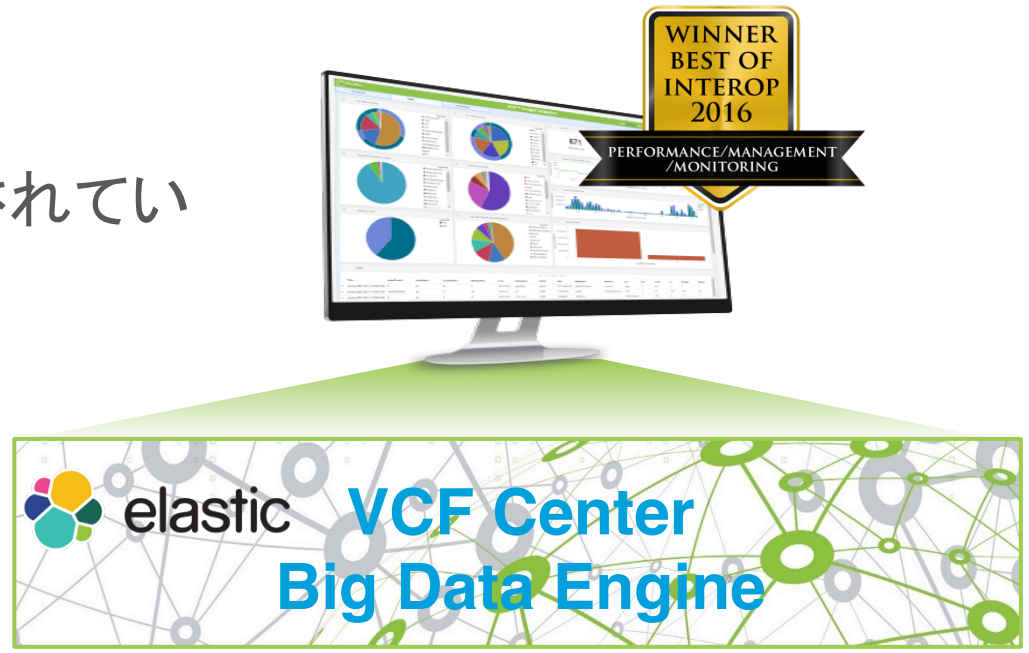
Edge Security Services Rack
- Grey vRouter for VTEP, Red vRouter to DC network Load Balancers
- Firewall on-a-stick in L2 mode for non-mission-critical traffic with bypass service option
- vFlow security ACL for N-S Policy Enforcement
- Pluribus VCF Analytics for mission-critical flow visibility

コネクションフローの分析

- ファブリックに合体している = デプロイが簡素化
- 常にON, ゼロタッチ = simple to use
- No sampling…every EAST-WEST connection
- TCP コネクションのステートがmachine tracking されている
- Tenant aware

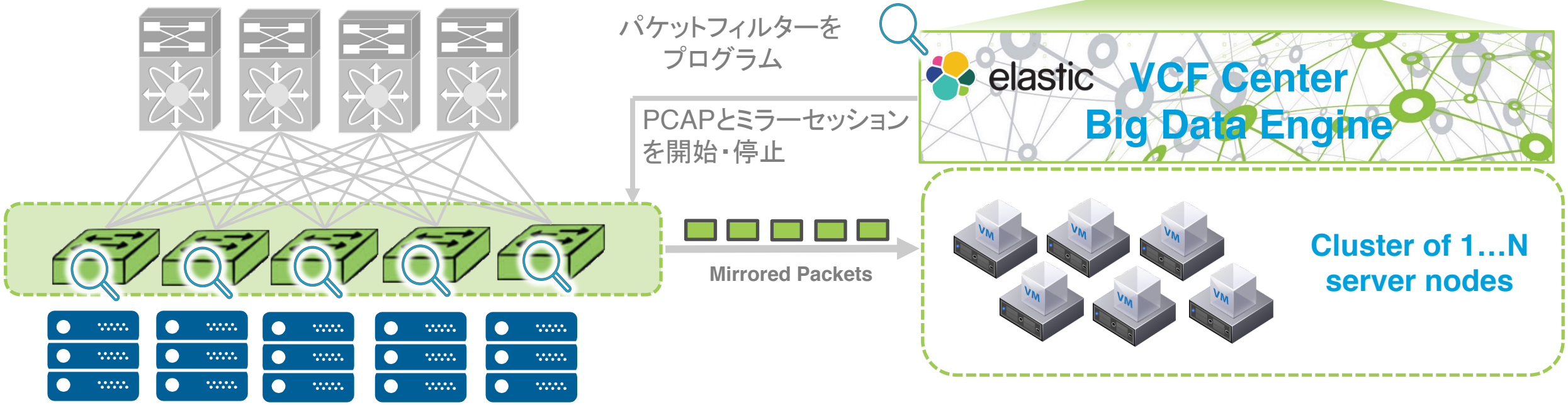


Flow Metadata



パケット分析

- オンデマンドパケットフィルタリング - L1-L4 header fields
- BroadcomチップにオフロードしてTerabit フィルタリング
- ミラーとPCAP ファイルを管理
- PCAPから抽出したパケットのメタデータを分析
- もしくは他から持ってきた PCAPファイルを分析

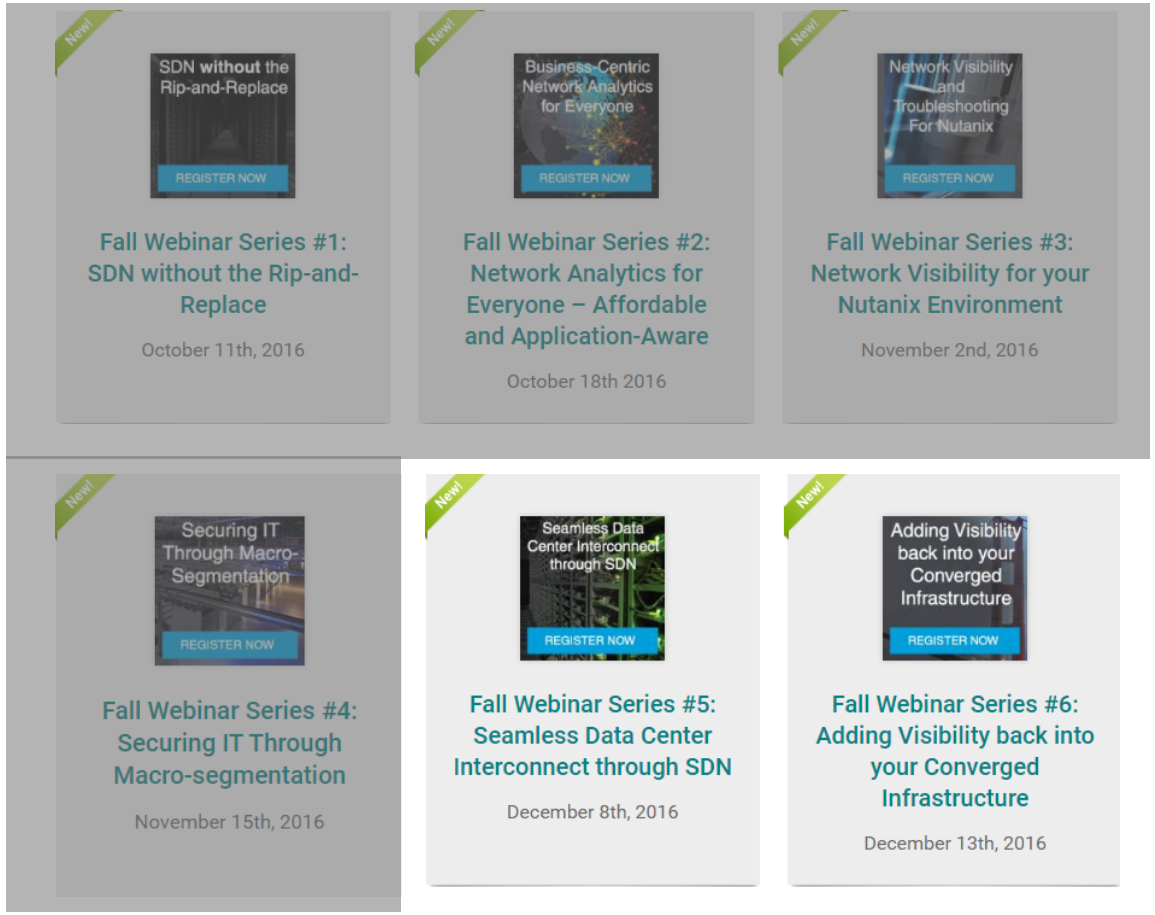


まとめ

1. マクロセグメンテーションでE-Wトラフィックをセキュアに
2. HW アクセレレーションでPhysical & Virtual に対応
3. マルチテナンシー全体を完全に隔離します
4. ポリシーを作って条件に基づいた細かいフローコントロール
5. 可視化と分析は継続的にポリシーの向上をもたらします

ご静聴ありがとうございました

ウェビナーからご覧いただけます



pluribusnetworks.com/resources/#webinars