Cisco ACI エンドポイント セキュリティ グループ（ESG）設計ガイド

目次

このドキュメントの目的

このドキュメント は、 Cisco® アプリケーション セントリック インフラストラクチャ（ACI®）エンドポイントセキュリティ グループ（ESG）ユース ケース と展開考慮について説明します。

前提条件

このドキュメントは、読者が Cisco ACI 技術の基本的な知識を持っていることを前提としています。Cisco ACI の詳細については、Cisco.com で入手可能な Cisco ACI ホワイト ペーパー を参照してください。

このドキュメントは ESG に焦点を当てており、詳細な契約構成と設計オプションについては説明していません。コントラクトの詳細について、[Cisco ACI コントラクト ガイド（Cisco ACI Contract Guide）]を参照します。

ESG 設定の詳細については、『Cisco APIC セキュリティ構成ガイド、リリース 6.0（x）』を参照してください。

用語

このドキュメントは、次の用語を使用します：

- TN：テナント
- VRF：仮想ルーティングおよび転送
- BD：ブリッジ ドメイン
- EPG：エンドポイント グループ – BD 内の 1 つ以上の VLAN に接続されたエンドポイントのコレクション
- ESG：エンドポイント セキュリティ グループ – VRF インスタンス内のエンドポイントのコレクション
- EP：Cisco ACI ファブリックに常駐するエンドポイント
- L3Out: レイヤ 3 外部または、外部ルーティング ネットワーク
- L3Out/外部 EPG：サブネット ベース EPG の L3Out
- ボーダー リーフ スイッチ: L3Out が展開されている Cisco ACI リーフ スイッチ
- VMware vCenter VMM ドメイン：VMware vCenter 上の仮想分散スイッチ （vDS）にマップする Cisco ACI 上の仮想マシン マネージャ ドメイン
- アプリケーション中心型設計とネットワーク中心型設計：
  - 一般的なネットワーク中心の設計では、ブリッジ ドメインごとに 1 つの EPG（セキュリティ グループ）が作成されます。通常、EPG には単一の VLAN 識別子が含まれており、これは従来のネットワーク設計に似ています。ネットワーク構成要素には、「epg-vlan-10、epg-vlan-11、epg-vlan-12」など、ネットワーク構成を反映した名前が付けられます。
  - アプリケーション中心の設計では、1 つ以上の EPG/ESG が同じブリッジ ドメインに作成されます。ネットワーク構成要素には、「epg-web、epg-app、epg-db」など、アプリケーションを反映した名前が付けられます。

図 1 は、このドキュメント全体で使用されるアイコンを示しています。オブジェクト ハンドルは、次の機能を表します：

- C：コントラクトの消費者
- CCI：消費されるコントラクト インターフェイス
- I: EPG / ESG 内契約

- P：契約業者

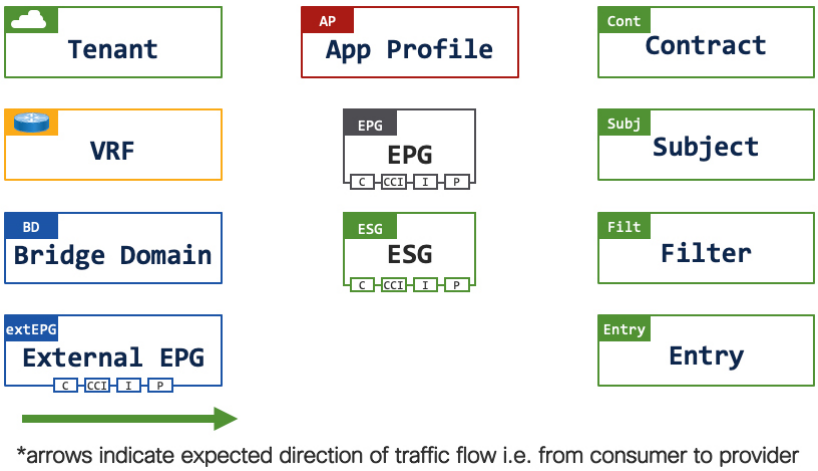


図 1. Cisco ACI アイコン

概要

このドキュメントでは、Cisco ACI リリース 6.0（2）までの機能について説明します。この資料は、複数のセクションに分けられます：

- ネットワーク中心からアプリケーション移行ストーリー：Pseudo Co は、ESG を初めて使用するユーザーのために Cisco ACI ファブリックで ESG を採用する一例を説明しています。
- ESG 設計例では、ESG に精通しているユーザー向けに、より多くの ESG 設計例を説明しています。
- 付録では、包括的な Cisco ACI マルチテナント設計例について説明します。

ネットワーク中心からアプリケーション中心への移行ストーリー：Pseudo Co

このセクションでは、サブネットごとに 1 つの EPG を使用するネットワーク中心の設計で、歴史的に Cisco ACI を使用していた疑似企業を使用した EPG から ESG への移行ストーリーについて説明します。

他の設計オプションについては、「ESG 設計例」セクションを参照してください。

疑似企業の Cisco ACI 導入の概要

疑似企業は、Cisco ACI ファブリックに直接接続されている ESXi ホスト上に多数の仮想マシン エンドポイントを持ついくつかの Cisco ACI テナントを構成しています。

次の図は、疑似企業の Cisco ACI ファブリックと接続されているデバイスの概要を示しています：

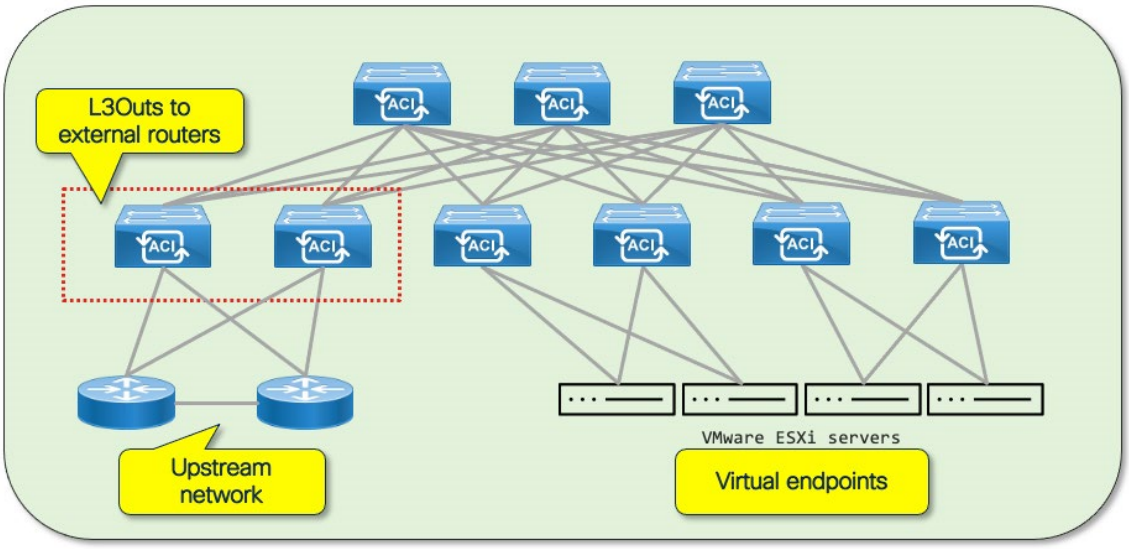


図 2. 疑似企業の Cisco ACI ファブリック: 物理トポロジ

ネットワーク導入

疑似企業は、ブリッジ ドメインから EPG への 1 対 1 のマッピングがあるネットワーク中心の設計と一般的に呼ばれる方法で Cisco ACI ファブリックを展開しました。ネットワーク実装の一環として、疑似企業は VMM ドメインを実装して、Cisco ACI ファブリックと ESXi ホスト間の VLAN の管理を簡素化することを選択しました。Cisco APIC VMM ドメインは、Cisco APIC の VLAN プールから vDS ポート グループに VLAN をダイナミックに割り当てます。ダイナミックな VLAN 割り当てのため、BD_name = EPG_name である命名形式を実装することが実用的であることがよくあります。ただし、このドキュメントの目的と、ブリッジ ドメインと EPG の機能を説明するために、このドキュメントでは、ブリッジ ドメイン名にサブネット CIDR を使用し、EPG 名に VLAN 識別子を使用します。

- テナント：デモ
- VRF：vrf-01
- ブリッジ ドメイン：10.0.1.0_24 – 10.0.7.0_24
- EPG：VLAN10 – VLAN70
- EP：さまざまなネットワーク セグメントに分散

次の図は、疑似企業のテナントの 1 つを表しています。

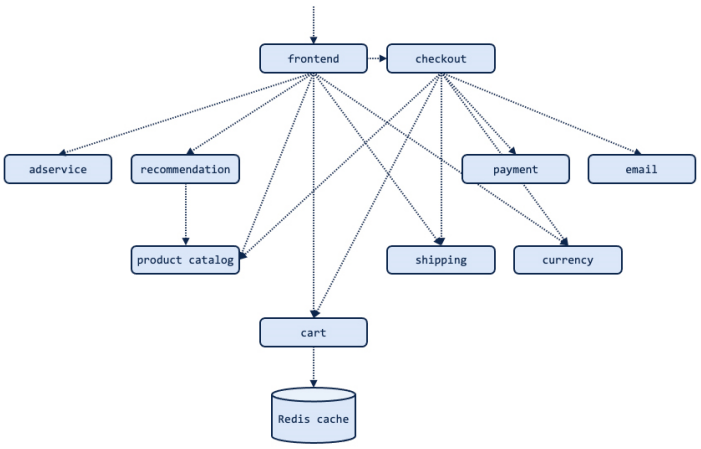
図 3. 疑似企業の Cisco ACI ファブリック：ネットワーク セグメント

参照アプリケーション

この設計ガイドでは、疑似企業が Cisco ACI ファブリックをネットワーク中心の設計からアプリケーション中心の設計に簡単に変換した方法を示します。以下の図は、この設計ガイド全体で使用される多層リファレンス アプリケーション（オンライン ブティック）を示しています。

注： リファレンス アプリケーションは、GitHub のこのデモ アプリケーションから着想を得たものです。

オンライン ブティック アプリケーションへのコンシューマ トラフィックは、添付の表に示すように、ポート 80/8080 でフロントエンド サービスを使用します。アプリケーション層の間の矢印は、送信元/コンシューマからターゲット/プロバイダーへの予想されるトラフィック フローの詳細を示しています。



Source/Consumer	Target/Provider	Target/Provider Port
cart	Redis cache	TCP 6379
checkout	cart currency email payment product catalog shipping	TCP 7070 TCP 7000 TCP 8080 TCP 50051 TCP 3550 TCP 50051
frontend	adservice cart checkout currency product catalog recommendation shipping	TCP 9555 TCP 7070 TCP 5050 TCP 7000 TCP 3550 TCP 8080 TCP 50051
outside	frontend	TCP 80/8080
recommendation	product catalog	TCP 3550

図 4. 疑似企業の Cisco ACI ファブリック：リファレンス アプリケーション

以下の図は、「デモ」テナント内のさまざまなネットワーク セグメント（サブネット）にオンライン ブティック アプリケーションがどのように展開されているかを示しています。フロントエンド、支払い、カートなどのいくつかのアプリケーション サービスは、異なるサブネットにまたがることに注意してください。疑似企業内の異なるサブネット間でのエンドポイントの分散が発生したのは、特定のアプリケーション層に必要なエンドポイントの数が指数関数的に増加したためです。特定のサブネット内での IP アドレスの枯渇が原因で、アプリケーション エンドポイントがサブネットの境界を超えています。

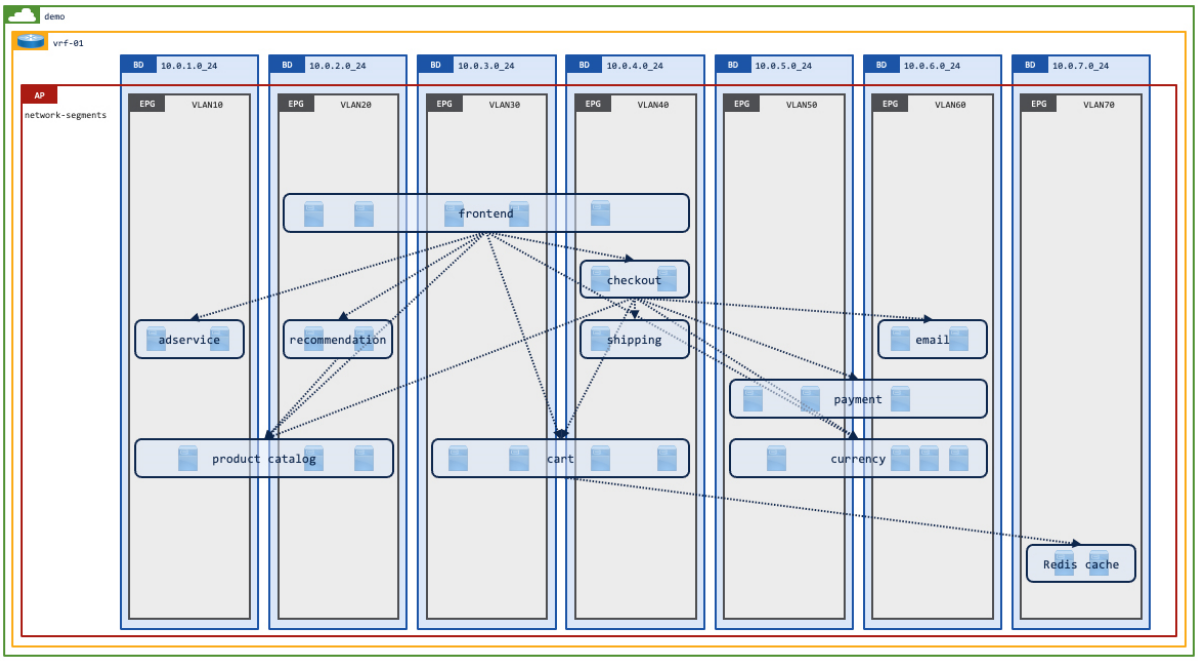


図 5. 疑似企業の Cisco ACI ファブリック：ネットワーク セグメント全体のリファレンス アプリケーション

疑似企業のネットワーク中心の Cisco ACI ファブリックでホストされるオンライン ブティック アプリケーションなどのアプリケーションでは、アプリケーションが正しく機能できるように、さまざまなアプリケーション層の間でオープンな通信が必要です。

Cisco ACI ファブリック上の多く/すべての EPG 間でオープンな通信を可能にするために使用できるいくつかの異なる構成オプションがあります。

- vzAny との契約: vzAny は、VRF インスタンス上のすべての EPG、ESG、および外部 EPG を表します。vzAny でオープンな「permit-any」コントラクトを提供および使用すると、VRF インスタンスのすべてのエンドポイント間でオープンな通信が可能になります。
- 優先グループ – 複数の EPG を優先グループに割り当てると、優先グループ内の EPG 間でオープンな通信が可能になりますが、VRF インスタンスごとに優先グループは 1 つだけという制限があります。
- セキュリティを無効にする – VRF インスタンスを「非強制」モードに設定すると、VRF インスタンスが「許可のみ」に変換され、VRF インスタンス内のすべてのエンドポイント間のオープン通信が許可されるため、このオプションはお勧めしません。セキュリティを無効にすると、セキュリティ コントラクトとサービス グラフなどの高度な機能が暗黙的に無効になります。

上記のオプションに加えて、Cisco ACI リリース 5.2（1g）以降では、ESG と EPG セレクタを使用して、複数の EPG を集約するセキュリティ グループを作成できます。デフォルトでは、特定の ESG 内の通信（ESG 内通信）が許可されています。EPG から ESG へのマッピングの使用例については、このセクションの後半で詳しく説明します。

疑似企業は現在、次の図に示すように、「共通」テナントからの「デフォルト」契約を提供および消費する vzAny を使用して、VRF インスタンス内でオープン通信を有効にしています。

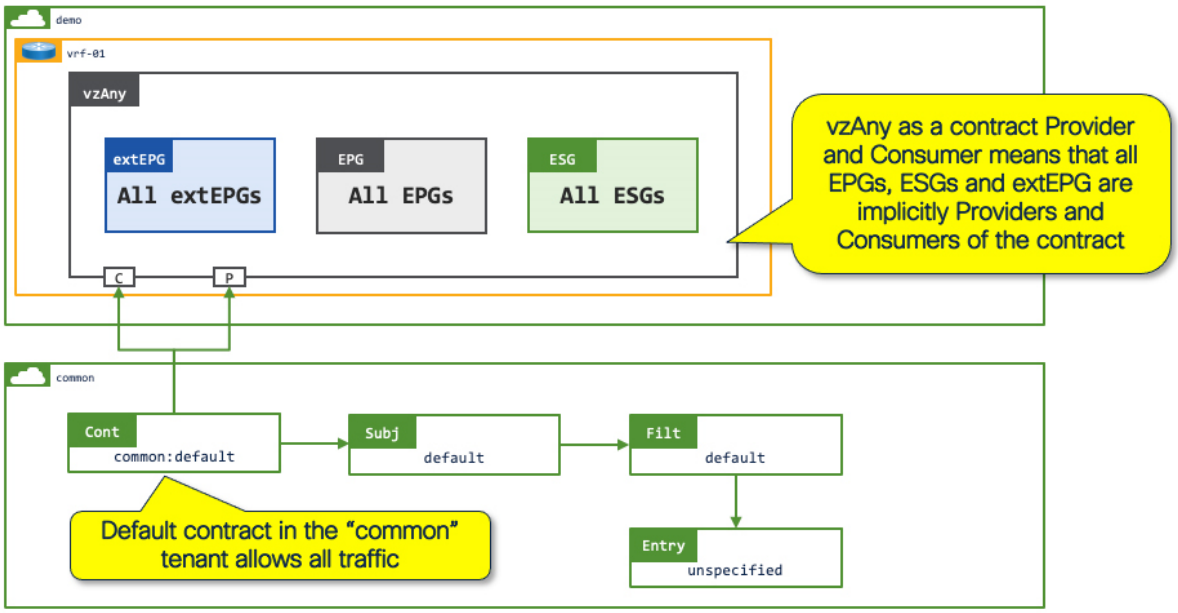


図 6. 疑似企業の Cisco ACI ファブリック：すべての EPG 間通信を許可する vzAny-to-vzAny 契約

エンドポイント グループとエンドポイント セキュリティ グループ

エンドポイント グループとエンドポイント セキュリティ グループの機能と設計に関する考慮事項を比較することが重要です。Cisco ACI の基本的なビルディング ブロック（下の図で詳しく説明）は、次のことを示しています。

- VRF インスタンス：単一のテナントにのみ存在できます。

- ブリッジ ドメイン：単一の VRF インスタンスにのみマッピングでき、1 つ以上のサブネット（セカンダリ IP アドレス）のルーティングを提供できます。
- EPG: ブリッジ ドメイン内のセキュリティ グループの境界を定義します。EPG へのアドミッションは、リーフ スイッチ（インターフェイス / VLAN）の静的パス バインディングまたは VMM バインディングによって定義されます。
- ESG：VRF インスタンス内のセキュリティ グループ境界を定義します。ESG への入学は、次のメソッドの 1 つ以上によって定義されます：
  - EPG セレクタ – 1 つ以上の EPG を ESG にマッピングできます
  - タグ セレクタ – エンドポイントは、以下に基づいて ESG にマッピングできます：
    - MAC アドレス
    - IP アドレス
    - VM 名
    - VM Tag
  - IP セレクタ– IP アドレスを ESG にマッピングできます。

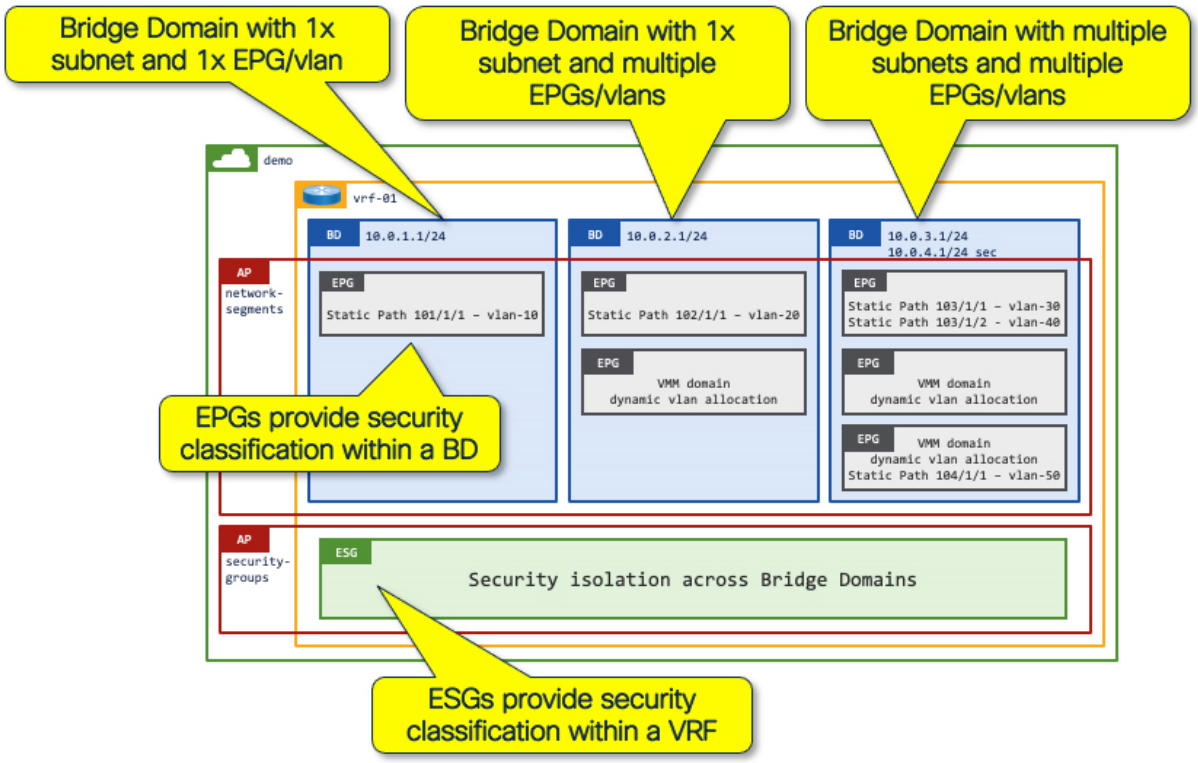


図 7. エンドポイント グループとエンドポイント セキュリティ グループのセキュリティに関する考慮事項

ESG マッピングは、セレクタの優先順位に関する FAQ の表に示されているように、スイッチおよびルーティングされたトラフィックの階層的な決定基準に基づいて実装されます。EPG セレクタに一致するエンドポイントは、タグ セレクタに一致するエンドポイントよりも低い一致優先度を持ちます。ESG 決定の選択により、ネットワーク管理者は、ネットワーク バッキングを変更することなく、エンドポイントを異なる ESG 間でダイナミックに移動できます。たとえば、EPG に含まれるすべてのエンドポイントは、EPG セレクタを使用して ESG-A にマ

ッピングできます。特定のエンドポイントは、より優先度の高いタグ セレクタを使用して ESG-B にマッピングできます。

要約すると、次のような柔軟なセキュリティ設計をサポートできるため、ESG を使用して Cisco ACI セグメンテーションを提供することをお勧めします。

- ESG によって定義されるセキュリティ グループは、単一のブリッジ ドメイン内のエンドポイント分類に限定されません。
- エンドポイントは、VLAN 識別子などの基盤となるネットワーク構成を変更したり、EPG を介してインターフェイスを変更したりせずに、セキュリティ グループ（ESG）を変更できます。

ESG 分類オプションの完全な詳細は、ESG 設計例のセクションで説明されています。

コントラクトの使用は EPG と ESG の両方に等しく適用できますが、ESG は、VRF インスタンス内の異なるブリッジ ドメインにまたがるエンドポイントのグループ化を可能にするため、強化されたセキュリティ オプションを提供します（上に示すように）。逆に、EPG は VRF インスタンス内の単一のブリッジ ドメインに関連付けられているため、異なるブリッジ ドメインにまたがるエンドポイントを選択することはできません。アプリケーション エンドポイントが異なる EPG およびブリッジ ドメインにまたがる場合、ネットワーク中心の設計からアプリケーション中心の設計に移行するときに、ブリッジ ドメインから EPG へのマッピングが障壁になる可能性があります（図 5）。ESG は、VRF インスタンス全体で動作するため、この制限を削除します。

設計のブループリント– アプリケーションごとの単一の ESG

疑似企業のネットワーク インフラ管理チームは、アプリケーションごとに 1 つのセキュリティ ゾーンを作成することにより、現在のネットワーク中心の設計からアプリケーション中心の設計に移行することを選択しました。最初の設計ブループリントでは、特定のアプリケーションのすべてのエンドポイントを 1 つの ESG に配置します。アプリケーションが ESG にマッピングされた後、チームは必要に応じて ESG メンバーシップを評価および調整します。たとえば、チームはデータベースなどの特定の共有サービスを専用の ESG に移動する場合があります。ESG 間のエンドポイントの移動は、ネットワーク バッキングを変更することなく、ESG 選択基準を調整するだけでシームレスに実現できます。

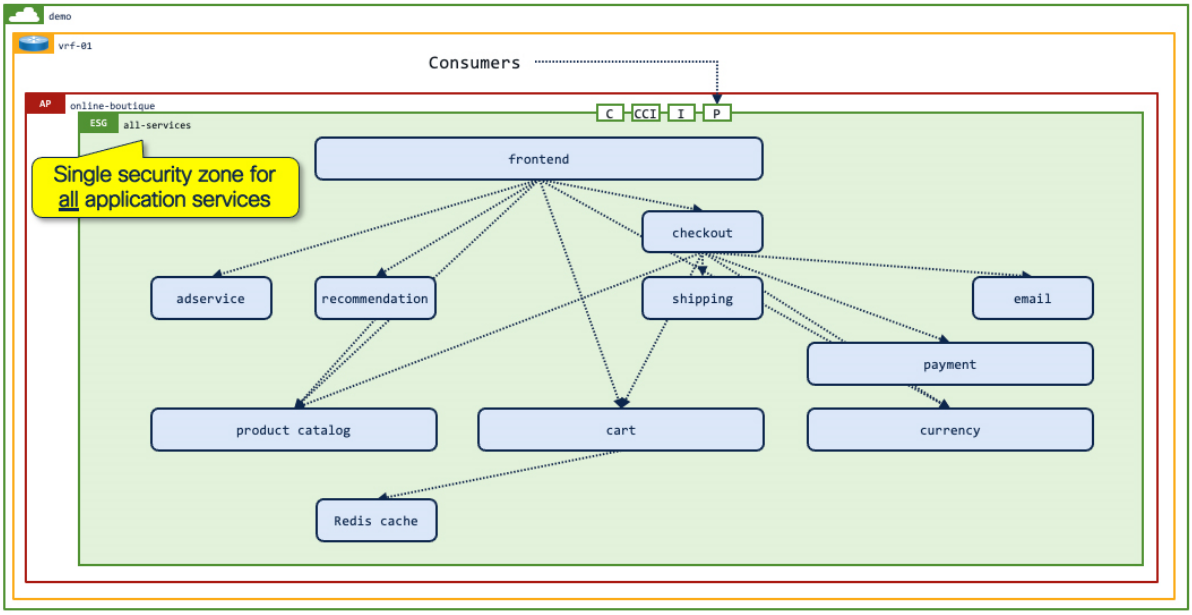


図 8. 疑似企業の Cisco ACI ファブリック：アプリケーションごとに 1 つの ESG（新しい設計）

アプリケーションごとに 1 つの ESG を実装すると、ネットワーク管理者は、アプリケーションが Cisco ACI ファブリックのどこで実行されているかを明確に把握できるようになり、次の主な利点が得られます。

- アプリケーションの可視性の向上：すべてのアプリケーション エンドポイントに対して単一の ESG を作成すると、ネットワーク管理者は、アプリケーション エンドポイントがネットワークのどこに接続されているかを正確に理解できます。含まれる詳細は次のとおりです：
  - MAC/IP アドレス
  - インターフェイス
  - VLAN カプセル化識別子
  - EPG
  - ポリシー タグ
  - VM 名 （読み取り / 書き込み VMM 統合が必要）
  - ホスティング サーバー（読み取り / 書き込み VMM 統合が必要）
  - レポート コントローラ（読み取り / 書き込み VMM 統合が必要）
  - VM タグ（読み取り / 書き込み VMM 統合が必要）
- ネットワーク セグメントではなくアプリケーションに関連付けられたセキュリティ：ESG により、ネットワークおよびセキュリティ管理者は、ネットワーク セグメントや IP アドレスではなくアプリケーションに基づいてセキュリティを実装できます。これにより、ルーティング パスにセキュリティ デバイスを挿入する必要がなくなるため、ネットワーク設計が簡素化されます。代わりに、レイヤ 4 からレイヤ 7 のサービス デバイスをアプリケーション内またはアプリケーション間にダイナミックに挿入できます（サービス グラフを使用）。

  - 契約の強化によるセキュリティの向上：Cisco ACI 契約は、提供 / 使用契約を使用するアプリケーション間、または ESG 内契約を使用する特定のアプリケーション内で、ステートレスなレイヤ 4 ハードウェア ベースの ACL セキュリティ制御を提供します。アプリケーションが識別され、そのエンドポイントが ESG にマップされたら、提供されたコントラクトで参照される（フィルタ）ポートを制限するか、TCP 接続が確立される方向を制御することによって、アプリケーションのセキュリティを強化できます。つまり、接続はコンシューマからプロバイダーへのみ確立できます。

  - 分離されたアプリケーション グループ：ESG は「強制」モード（ESG 内分離）に設定できます。これにより、ESG 内のすべてのトラフィックがブロックされ、アプリケーション エンドポイントが分離されます。必要に応じて、ESG 内の特定のポートでの通信を許可するために、ESG 内の契約を ESG に追加できます。

  - インテリジェントなサービス挿入: レイヤ 4 からレイヤ 7 サービスは、アプリケーション ESG の前または ESG 内のいずれかにダイナミックに挿入できます。たとえば、サービス グラフ との ESG 内コントラクトを隔離された ESG に追加して、NGFW / IPS を介してすべてのエンドポイント内トラフィックをリダイレクトできます。
- アプリケーションの依存関係のマッピング: ネットワーク管理者は、ESG 内の契約を利用して、サービス グラフを介して ESG 内のすべてのトラフィックを、ファイアウォールなどのレイヤ 4 からレイヤ 7 のサービス デバイスに転送できます。「`permit-any | log`」ルールを使用してファイアウォールを構成すると、ファイアウォールは ESG 内のすべてのエンドポイント間通信に対して syslog メッセージを生成できます。さらに、サービス グラフを使用して、ESG 宛てのトラフィックをレイヤ 4 からレイヤ 7 のサービス デバイスにリダイレクトして、アプリケーションへのすべてのトラフィックをログに記録することもで

きます。**注：**Cisco ACI 契約のログを有効にすることもできます。ただし、ロギングは、拒否されたトラフィックの場合は 500pps、許可されたトラフィックの場合は 300pps に制限されています。

- 監査機能の改善：Cisco ACI ファブリックでアプリケーション エンドポイントを表示する機能により、ネットワーク管理者は、アプリケーション、関連するセキュリティ ルール、およびレイヤ 4 からレイヤ 7 のサービス統合を監査するための合理化されたアプローチが提供されます。
- トラブルシューティングの改善：Cisco ACI ファブリックでアプリケーションを表示する機能により、ネットワーク管理者は個々のアプリケーションの正常性を表示できるため、アプリケーション パフォーマンスの問題をパケット ドロップなどの潜在的なネットワーク エラーとすばやく簡単に関連付けることができます。

次の図は、特定の ESG の Cisco APIC で利用可能な運用情報の詳細を示しています。

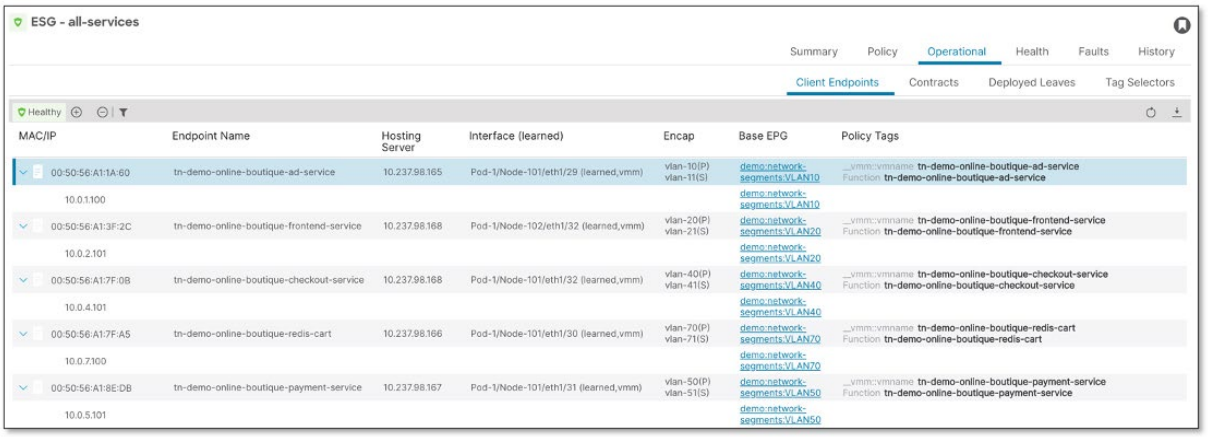


図 9. ESG の可視性（運用タブ）

移行手順

疑似企業は、ネットワーク中心の設計からアプリケーション中心の設計に変換するために必要な次の手順を特定しました：

1. EPG セレクタを使用して EPG から ESG へのマッピングを導入し、特定の VRF インスタンスの EPG 間のオープンな通信を許可します。これにより、vzAny コントラクトの要件がなくなり、将来的により柔軟なセキュリティ オプションが可能になります。
2. タグ セレクタによる VM タグ識別子を使用して、オンライン ブティック仮想マシン エンドポイントに単一の ESG を実装します。
3. オンライン ブティック アプリケーション ESG とネットワーク上の他の ESG との間の契約を使用した通信を許可します。
4. オンライン ブティック アプリケーション ESG に対して開いているプロトコルとポートを選択して、セキュリティを強化します。

前に詳しく説明したように、疑似企業は、vzAny で提供および使用される単純な「すべて許可」コントラクトを導入しました。ネットワーク中心の設計からアプリケーション中心の設計への移行中は、vzAny によって提供されるオープンなセキュリティ コントロールを変更しないでください。現在のオープンなセキュリティ コントロールを維持できないと、アプリケーション接続の問題が発生する可能性があります。後の段階で、疑似企業は、契約で定義されたオープン アプリケーション セキュリティ ルールがセキュリティの観点から十分であるかどうかを

判断できます。より厳密なセキュリティが必要な場合は、アプリケーションに必要なプロトコル/ポートを指定するだけでこれを実現できます。

ステップ 1：サブネット間のオープン通信用に単一の ESG を実装する（EPG セレクター）
疑似企業は、図 3 に示すように、ブリッジ ドメインと EPG 間の 1:1 マッピングを使用して、典型的なネットワーク中心の設計で Cisco ACI ネットワークを実装しました。各ブリッジ ドメインは、エンドポイント用の単一のサブネット / デフォルト ゲートウェイで構成され、VLAN バッキングを提供する単一の EPG にマップされます。EPG へのエンドポイントの分類は、着信リーフ / インターフェイス / VLAN のトラフィックを照合することによって実行されます。

ネットワーク中心からアプリケーション中心への移行の一環として、疑似企業は、すべてのサブネット / EPG 間のオープンな通信を提供する単一の ESG を実装します。次の図をご覧ください：

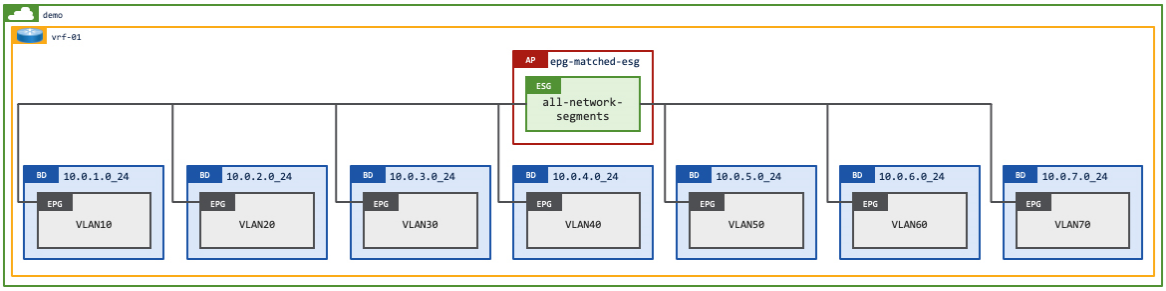


図 10. 疑似企業の Cisco ACI ファブリック：複数の EPG に対する単一のセキュリティ ゾーン

EPG セレクタを使用した複数の EPG の単一の ESG へのマッピングは、Cisco ACI ファブリック上の複数の EPG 間の通信を可能にする代替ソリューションです。EPG から ESG へのマッピングは、優先グループを使用するよりも柔軟なソリューションです。Cisco ACI は、VRF インスタンスごとに複数の ESG をサポートしますが、VRF インスタンスごとに 1 つの優先グループしか存在できません。さらに、優先グループ自体に契約を適用して、優先グループのすべての EPG メンバーから優先グループ外の別の EPG への通信を許可することはできませんが、契約を ESG に直接適用することはできます。

vzAny を使用するより、ネットワーク管理者にマップするための特定の EPG を選択させることを許可するため、複数の EPG から ESG へのマッピングも、vzAny と比較してより優れたセキュリティ設計であると考えられています。これは VRF インスタンス内の EPG、ESG、と外部 EPG を暗黙的に選択します。

ネットワーク管理者は、1 つ以上の EPG を ESG にマッピングすると、EPG のクラス識別子の変更がトリガーされることに注意する必要があります。EPG を ESG にマッピングする前に、VRF インスタンスの各 EPG には一意のクラス識別子があります。EPG を ESG にマッピングすると、マッピングされた各 EPG のクラス識別子が ESG のクラス識別子に書き換えられます。すべてのエンドポイントが同じクラス識別子を持つ ESG に分類されるようになったため、すべてのトラフィックは契約なしで暗黙的に許可されます。

注：　クラス識別子の再分類により、ネットワーク トラフィックが一時的に低下します。変更ウィンドウ中に EPG から ESG へのマッピングを実行することをお勧めします。

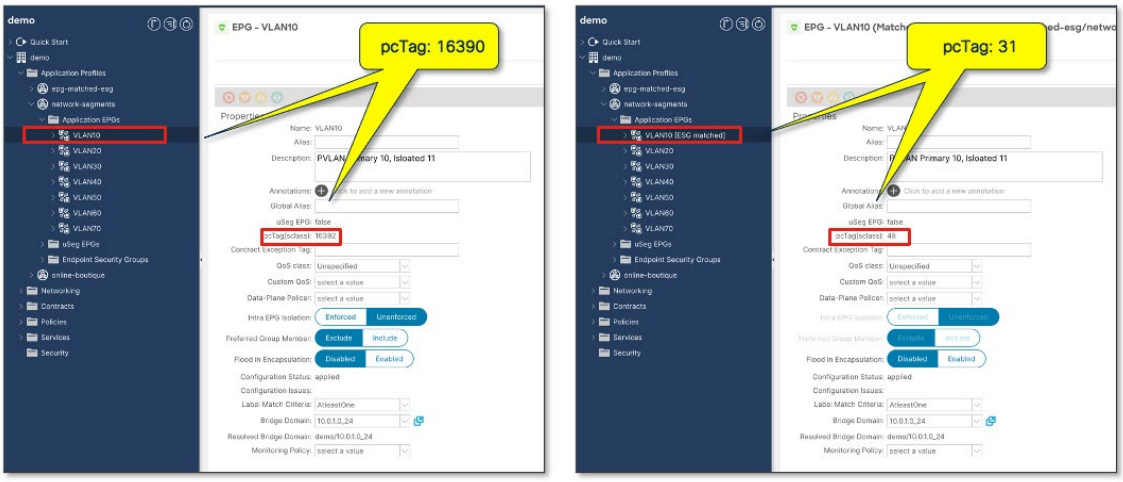


図 11. 疑似企業の Cisco ACI ファブリック: EPG から ESG への移行（クラス識別子の変更）

EPG セレクタは、VRF インスタンス内でオープンな通信を許可する vzAny とは対照的に、EPG 間の契約ですでに展開されている Cisco ACI ファブリックなど、より高度な移行シナリオにも役立ちます。このようなシナリオでは、EPG から ESG に移行する際に、これらの契約とセキュリティ グループを保持する必要があります。詳細な手順については、『Cisco APIC セキュリティ構成ガイド』の「エンドポイント セキュリティ グループ > ESG 移行戦略」を参照してください。

EPG セレクタの構成

以下の図は、構成を示しています：ロケーションは、テナント > アプリケーション プロファイル > Application_Profile_name > エンドポイント セキュリティ グループ > ESG_name > セレクタ > EPG セレクタになります。

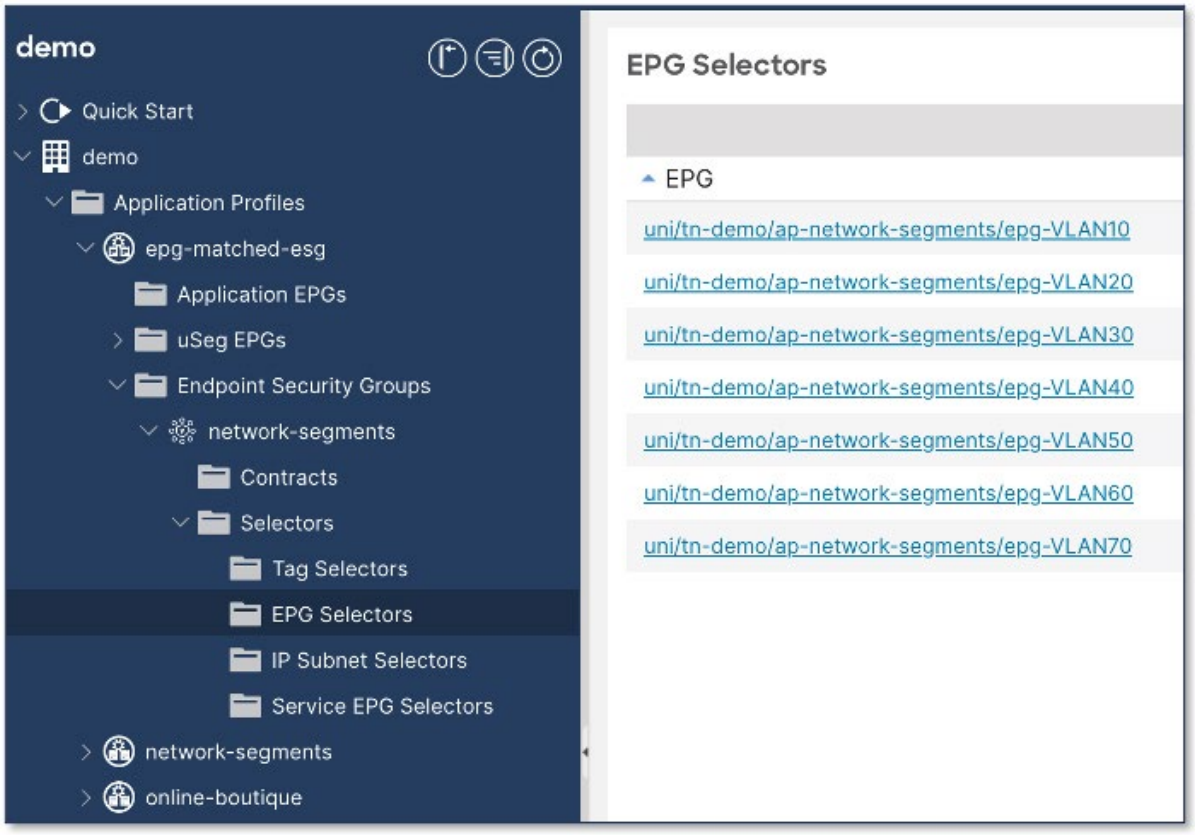


図 12. EPG セレクタ

注： 同じ VRF インスタンス内のエンドポイントはすべて、同じ ESG に属することができます。ただし、EPG セレクタを使用して ESG を構成する場合、EPG は ESG と同じテナントに属している必要があります。

ステップ 2：1 つのアプリケーションのすべてのエンドポイント（タグ セレクター）に 1 つの ESG を実装する

疑似企業のアプリケーション所有者は、特定のアプリケーションを構成するワークロードを簡単に識別できるように、VMware vCenter のアプリケーション仮想マシンにタグを割り当てています。Cisco ACI は、割り当てられた仮想マシン タグを VMware vCenter から収集し、それらを Cisco APIC の ESG タグ セレクタにマッピングすることで活用できます。

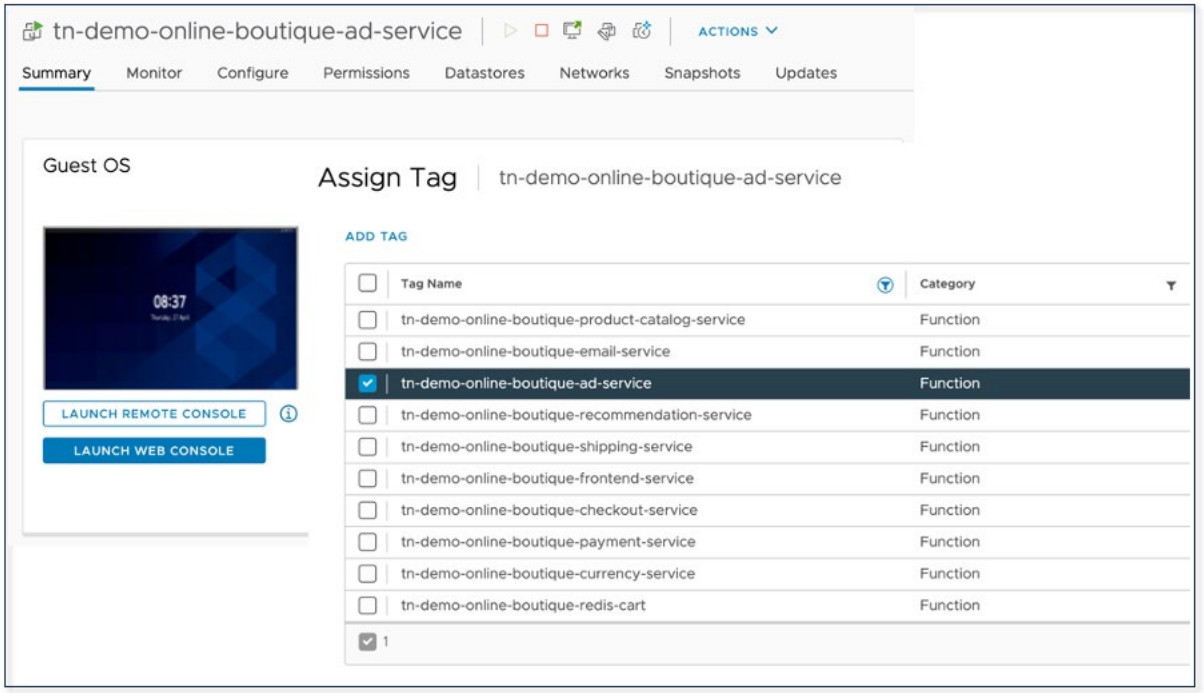


図 13. 仮想マシンのタグ割り当て

VMware vCenter の仮想マシン タグを Cisco APIC の Cisco ACI タグに一致させることにより、ネットワーク管理者とアプリケーションの所有者は、仮想マシンを元の「すべてのネットワーク セグメント」の ESG（図 10 に示す）からシームレスかつダイナミックに移動できます。「online-boutique:all-services」アプリケーション ESG を修正します。このステップでは、単一のアプリケーション（オンライン ブティック）に焦点を当てていますが、VRF インスタンス内に複数の ESG を作成する機能により、ネットワーク管理者は、図 20 に示すように、アプリケーションごとに 1 つ（または複数）の ESG を使用して、同じ VRF インスタンスに複数のアプリケーションを含めることができます。

注： 仮想マシン タグを持つタグ セレクタは、EPG セレクターよりも優先されます。この優先順位により、VRF インスタンス上の異なる ESG 間でエンドポイントをダイナミックに移動できます。セレクタの優先順位の詳細については、FAQ のセレクタの優先順位の順序を参照してください。

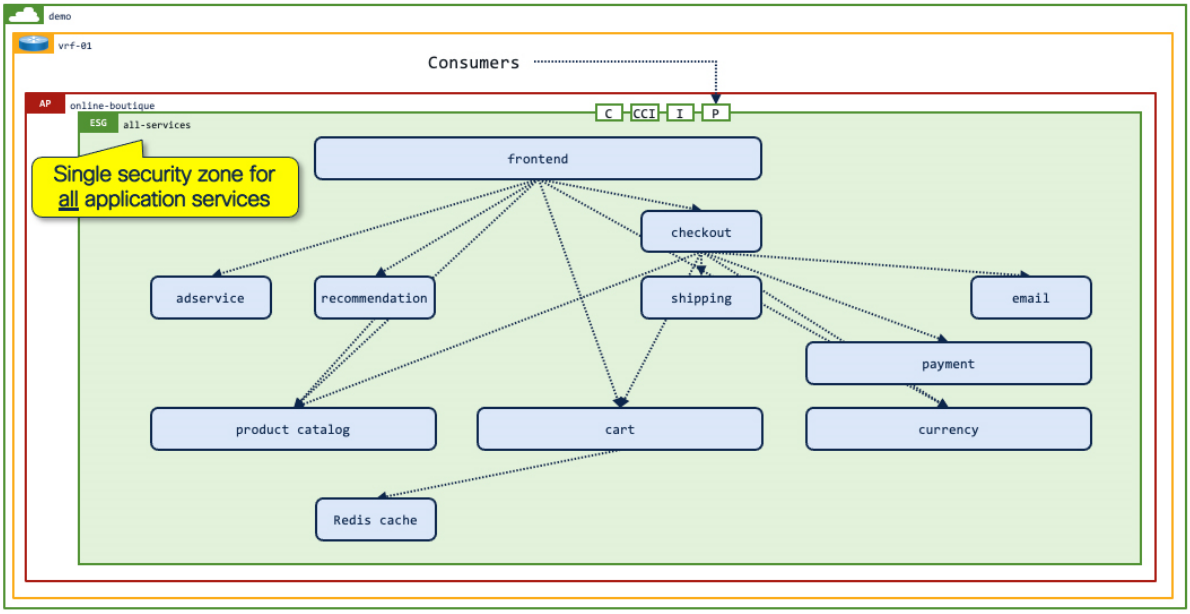


図 14. 単一の ESG 内のすべてのアプリケーション エンドポイント

タグセレクタに基づく分類

次の図は、タグ セレクタを作成するための構成オブジェクトを示しています。

ロケーションは、テナント > アプリケーション プロファイル > Application_Profile_name > エンドポイント セキュリティ グループ > ESG_name > セレクタ > タグ セレクタになります。

Cisco ACI タグ セレクタ（下）は、仮想マシンの**機能**が特定の**タグ値**と**等しい** VMware vCenter 上の仮想マシンタグと一致します。

例： 機能 = tn-demo-online-boutique-currency-service – このキー/値ペアは、テナント「demo」の「online-boutique」アプリケーションの一部として「通貨サービス」を提供する仮想マシンに一致します。

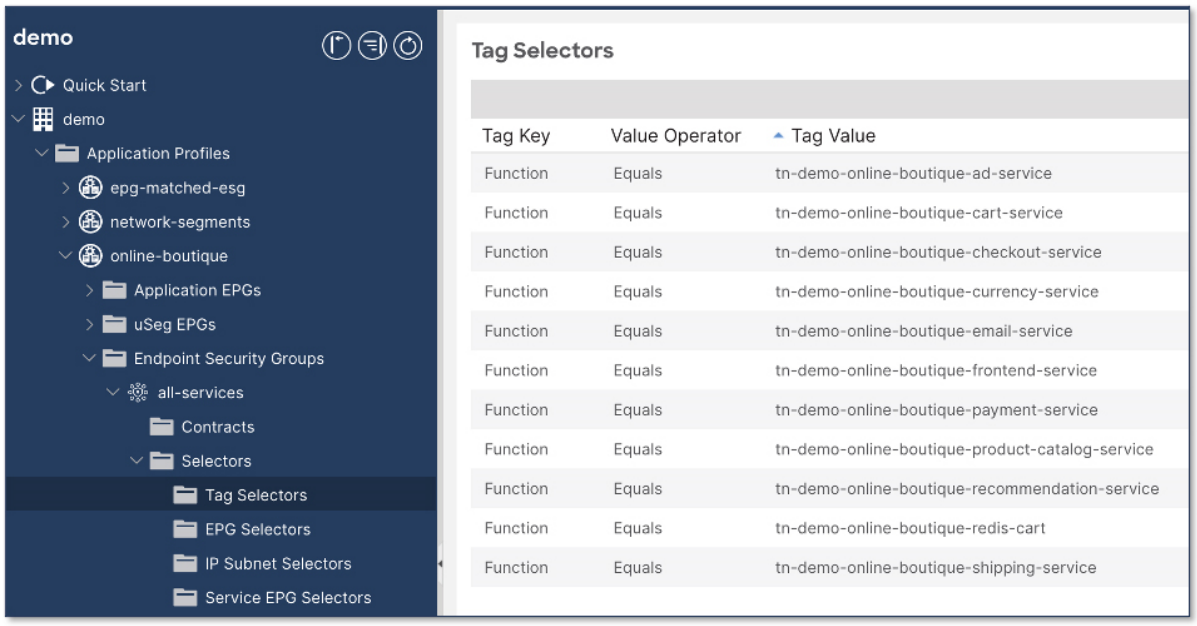


図 15. 疑似企業の Cisco ACI ファブリック：VM タグ付きの一連の EPG に 1 つの ESG

ESG マッピングに VM タグを使用するには、構成が次の前提条件を満たしている必要があります。

- VMM ドメインでタグ コレクションを有効にします。
- VMM ドメインを使用して、EPG でマイクロセグメンテーションを有効にします。

前提条件：VMM ドメインでタグ コレクションを有効にする
VMware タグ セレクタで ESG を使用する場合は、VMM ドメインの「タグ コレクションを有効にする」ボックスにチェックを入れる必要があります。

以下の図は、構成を示しています。ロケーションは、仮想ネットワーク > VMware > ドメイン名 > 全般にあります。

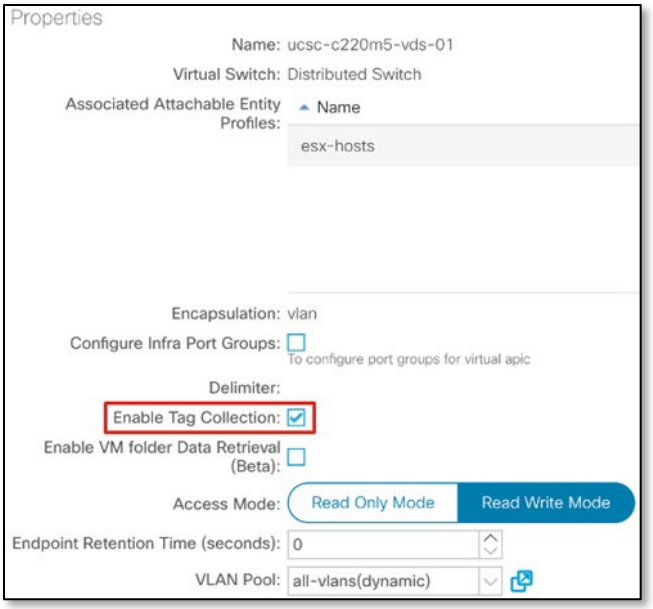


図 16. 前提条件：VMM ドメインで「タグ コレクションを有効にする」

前提条件：VMM ドメインを持つ EPG でマイクロ セグメンテーションを有効にする

VMware vDS VMM ドメインで ESG を使用する場合は、VMM ドメインに関連付けられた EPG の「マイクロセグメンテーションを許可する」ボックスにチェックを入れて、VM タグまたは VM 名によってエンドポイントを選択できるようにする必要があります。EPG が ESG（EPG セレクタ）に直接マッピングされている場合、EPG から ESG へのマッピングは EPG VLAN に基づいているため、「マイクロセグメンテーションを許可する」を設定する必要はありません。

「マイクロセグメンテーションを許可する」ボックスにチェックを入れると、EPG のポート グループに PVLAN（プライベート VLAN）が構成されます。既存の VMM マッピングされた EPG を再構成すると、vDS は ダイナミック VLAN プールからの新しい PVLAN ペアで動的に更新されます。レイヤ 2 マルチキャストまたはフラッディング トラフィックが必要な場合は、例 12: L2 マルチキャスト を使用した ESG のセクションを参照してください。

注：　「マイクロセグメンテーションを許可する」ボックスは、デフォルトではチェックされていません。

以下の図は、構成を示しています：ロケーションは、テナント > アプリケーション プロファイル > Application_Profile_name > アプリケーション EPG > EPG_name > ドメインにあります。

Cisco ACI リーフ スイッチと ESXi ホストの間に中間スイッチ（ブレード スイッチなど）があるネットワーク展開の場合、ネットワーク管理者は、VMM ドメインで使用される PVLAN ペアを静的に定義する必要があります。割り当てられた VLAN は、中間スイッチでも構成する必要があります。PVLAN ペアは Cisco ACI でダイナミックに割り当てることができますが、これにより、管理者が中間スイッチで同じ PVLAN ペアのセットを手動で構成することが難しくなる場合があります。Cisco ACI で PVLAN ペアを静的に定義する場合、VLAN 識別子は、VMM ドメインに関連付けられた VLAN プール内の静的 VLAN 範囲から割り当てる必要があります。

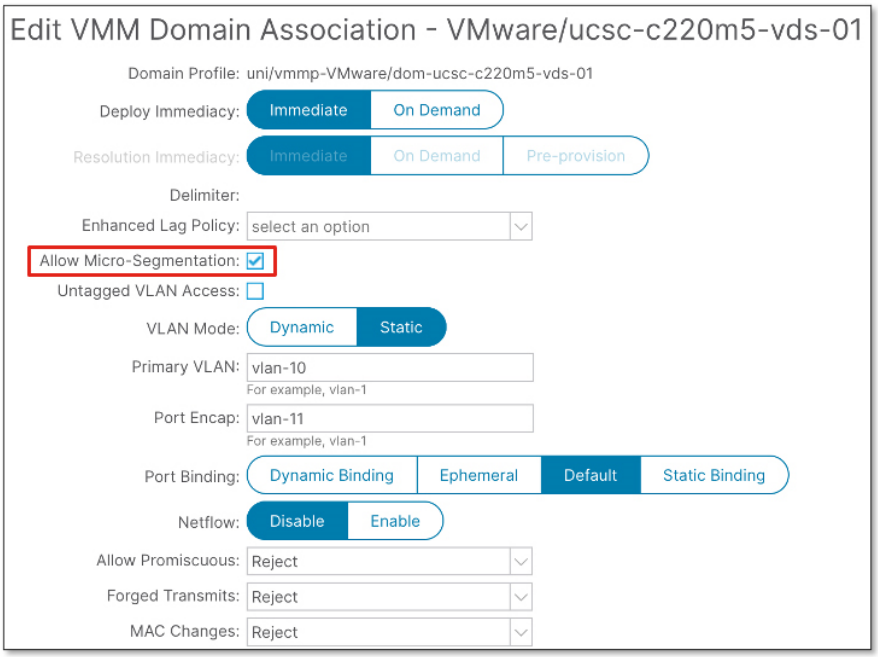


図 17. 前提条件：直接接続されたホストの EPG で「マイクロセグメンテーションを許可する」 – 中間スイッチが展開されている場合は、静的 VLAN 割り当てが推奨されます。

タグ セレクタを構成

次の手順では、タグ セレクタを使用して ESG を構成し、ESG に属する仮想マシンのエンドポイントを定義します。

以下の図は、構成を示しています：ロケーションは、テナント > アプリケーション プロファイル > Application_Profile_name > エンドポイント セキュリティ グループ > ESG_name > セレクタ > タグ セレクタになります。

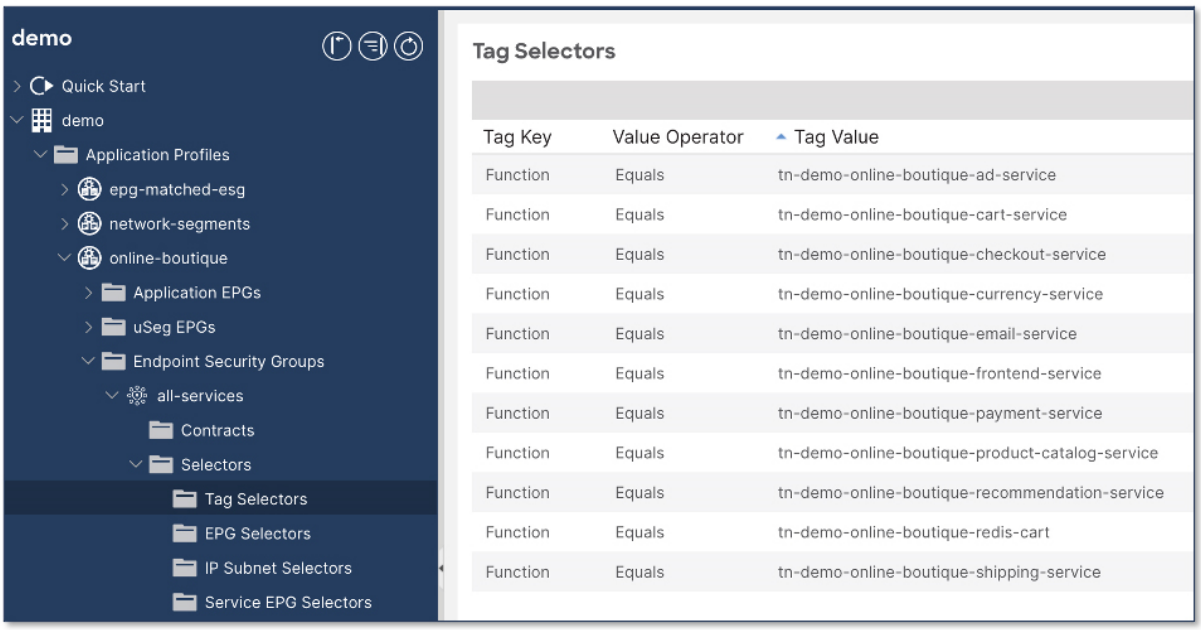


図 18. VM タグセレクタ

次の VMM 情報は、サポートされています：

- VM 名（タグ キー：__vmm::vmname、タグ値：<VM name>））
- vSphere VM タグ（タグ キー:<category>、タグ値：<tag name>）

次の例では、Cisco APIC が VM 名（vmm::vmname）と vSphere VM タグを VMware vCenter から取得しています。次に、Cisco APIC はそれらを VM の MAC アドレスに割り当てました。Cisco APIC は、vSphere タグを Cisco APIC タグ セレクタに一致させました。ブリッジ ドメインと VRF インスタンスは、Cisco APIC エンドポイント マッピング データベースから識別されます。

注： Cisco APIC は、5 分のタイム ウィンドウに 1 回、VMware vCenter からタグを読み取ります。

Cisco APIC GUI の場所は、テナント > ポリシー > エンドポイント タグ > エンドポイント MAC です。

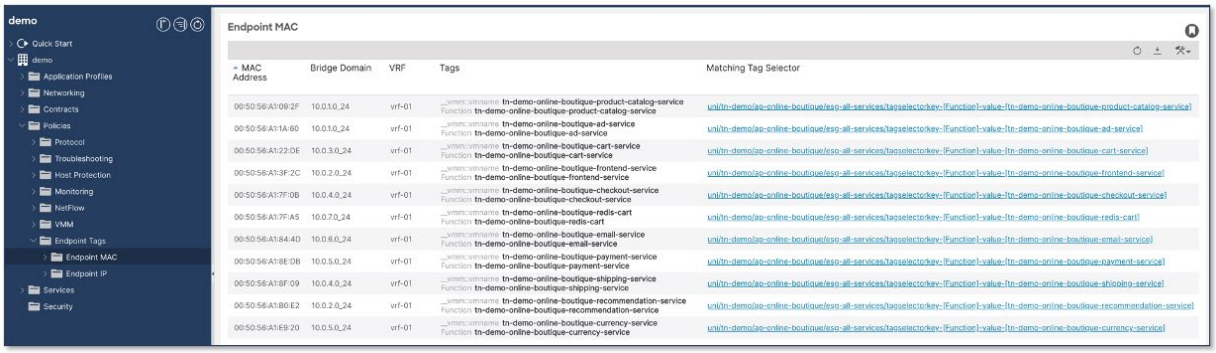


図 19. ポリシー タグ：エンドポイント MAC

ステップ 3：アプリケーション間通信（ESG 間契約）

アプリケーションのエンドポイントが 1 つの ESG にグループ化されたら、より広いネットワークから（コントラクトを使用して）アプリケーションへのアクセスを提供する必要があります。

以下の例では、オンライン ブティック アプリケーション（online-boutique:all-services ESG）は、「permit-to-tn-demo-online-boutique」契約を使用するどんなリモート サブネットからの application-monitoring:all-services ESG、 all-network-segments ESG と remote-users 外部 EPG に消費されるサービス（契約プロバイダ）を提供します。

online-boutique:all-services ESG は、core-services:all-services ESG からのアクティブ ディレクトリ、DNS、NTP、ソフトウェア更新などのサービスも使用します。

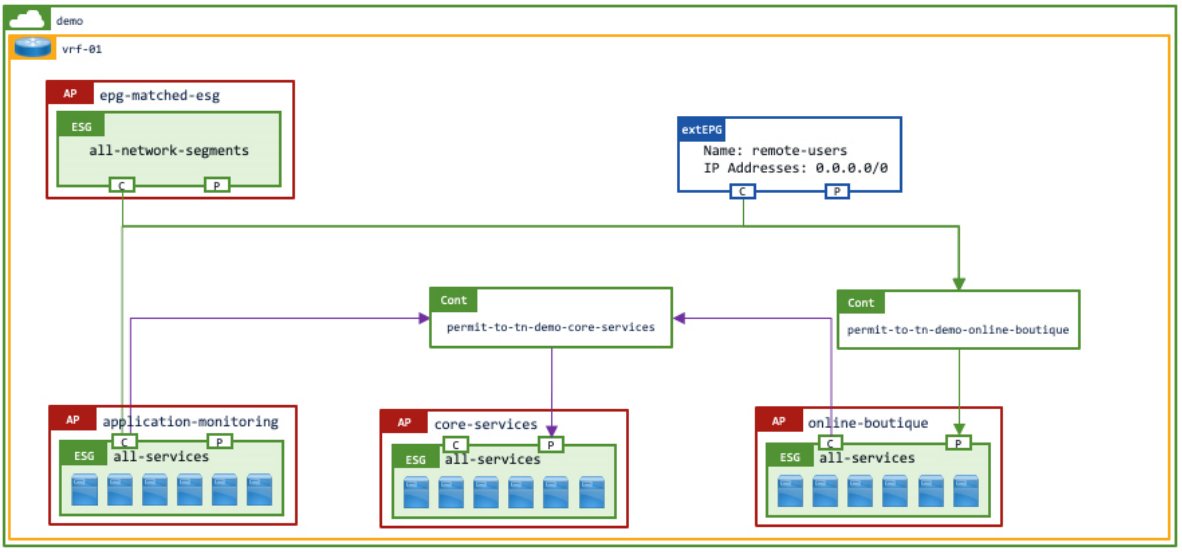


図 20. 疑似企業 Cisco ACI ファブリック： ESG 間の契約

矢印は、消費者からプロバイダーへの予想されるトラフィック フローを示しています。

表 1 契約関係

消費者 ESG	契約名	プロバイダー ESG
epg-matched-esg：all-network-segments	permit-tn-demo-online-boutique	online-boutique：all-services
application-monitoring：all-services	permit-tn-demo-online-boutique	online-boutique：all-services
extEPG：remote-users	permit-tn-demo-online-boutique	online-boutique：all-services
online-boutique：all-services	permit-tn-demo-core-services	core-services：all-services
application-monitoring：all-services	permit-tn-demo-core-services	core-services：all-services

ESG 間の契約を構成することにより、特定の ESG 間トラフィックのみが許可されます。さらに、ESG 内トラフィックはデフォルトで許可されます。「デフォルト」の permit-any フィルタを使用する代わりに、より詳細なフィルタを使用して、ESG 間トラフィックに対してのみ特定のタイプのトラフィックを許可することができます。詳細については、[ACI 契約ガイド（ACI Contract Guide）] を参照します。

[手順 4：追加のアプリケーション セキュリティを適用する（Step 4: Enforce additional application security）]

ESG 内の隔離または契約

ESG 内の通信はデフォルトで「すべて許可」ですが、追加のセキュリティ施行を ESG に適用して、ESG 内の「すべてを拒否」トラフィックまたは「特定のポートを許可」することができます。トラフィックを「すべて拒否」するには、ESG で Intra-ESG の隔離を強制に設定する必要があります。「特定のポートを許可する」には、ESG 内契約を ESG に追加する必要があります。ESG 内コントラクトは、サービス グラフを利用して、次世代ファイアウォール/IPS などのレイヤー 4 からレイヤー 7 のサービス デバイスにトラフィックをリダイレクトできます。

以下の例では、 online-boutique:all-services ESG のすべてのエンドポイントが自由に通信できます。ただし、監視サーバー間のエンドポイント間通信の要件がないため、application-monitoring:all-services ESG のエンドポイント間の通信はブロックされます。

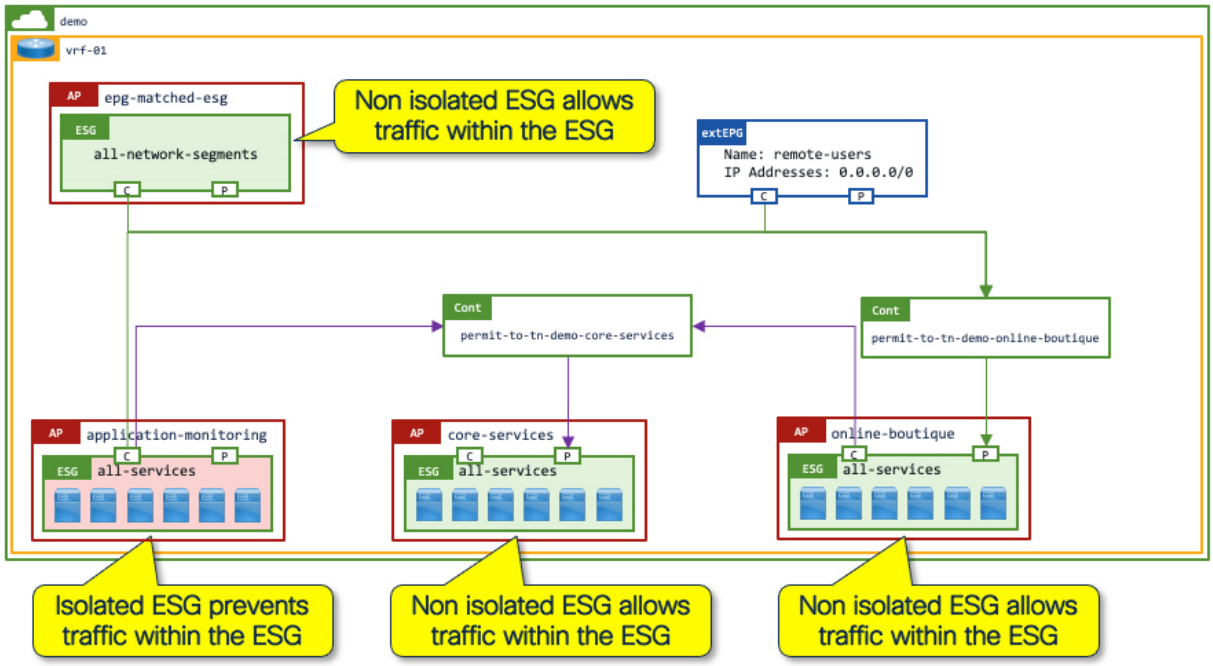


図 21. 疑似企業の Cisco ACI ファブリック: ESG 内分離

次の図は、ESG 内の分離構成を表示しています。デフォルトでは、ESG 内の分離は強制されません。ロケーションは、テナント > アプリケーション プロファイル> Application_Profile_name > エンドポイント セキュリティ グループ > ESG_name > ポリシー > 全般にあリマス。

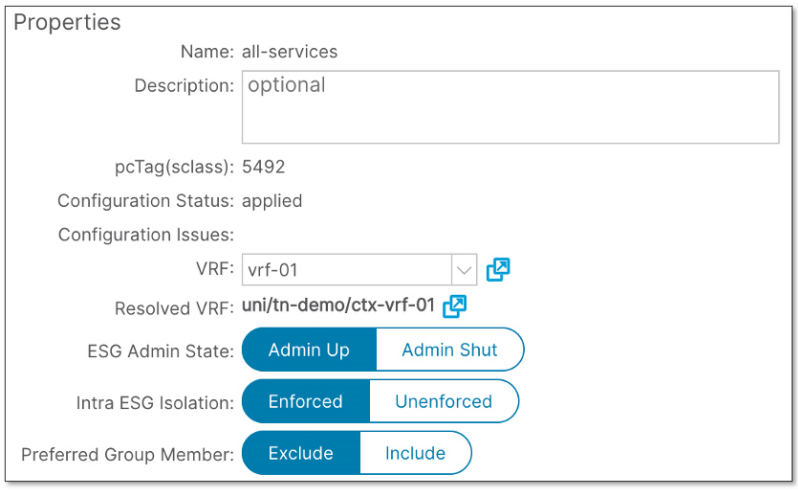


図 22. 疑似企業の Cisco ACI ファブリック：ESG 内分離（強制）

以下の図は、ESG 内の契約構成を示しています。場所は、テナント > アプリケーション プロファイル > Application_Profile_name > エンドポイント セキュリティ グループ > ESG_name > 契約 > Intra-ESG 契約の追加にあります。

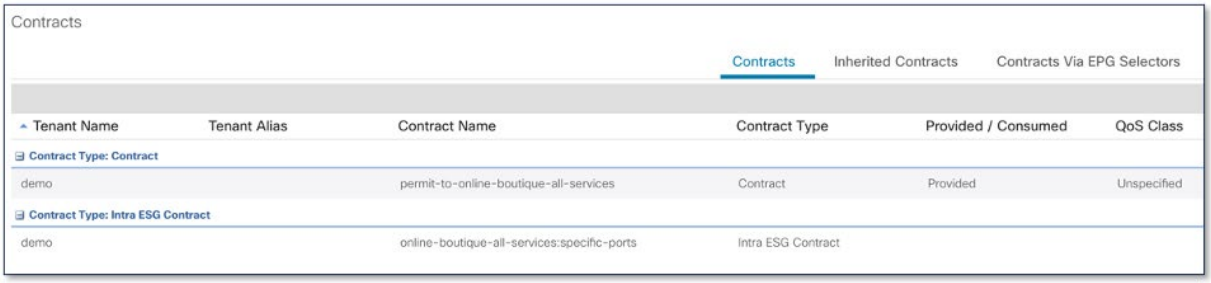


図 23. 疑似企業の Cisco ACI Fabric：ESG 内契約

レイヤ 4 からレイヤ 7 へのサービス挿入のための PBR を使用したサービス グラフ

ステートレス フィルタリングを備えたコントラクトを使用したハードウェア ベースの許可/拒否セキュリティの実施に加えて、ファイアウォールや IPS（侵入防御システム）などのステートフル レイヤ 4 からレイヤ 7 デバイスを、ESG 間または ESG（イントラ ESG）内のデータ パスにダイナミックに挿入することもできます。

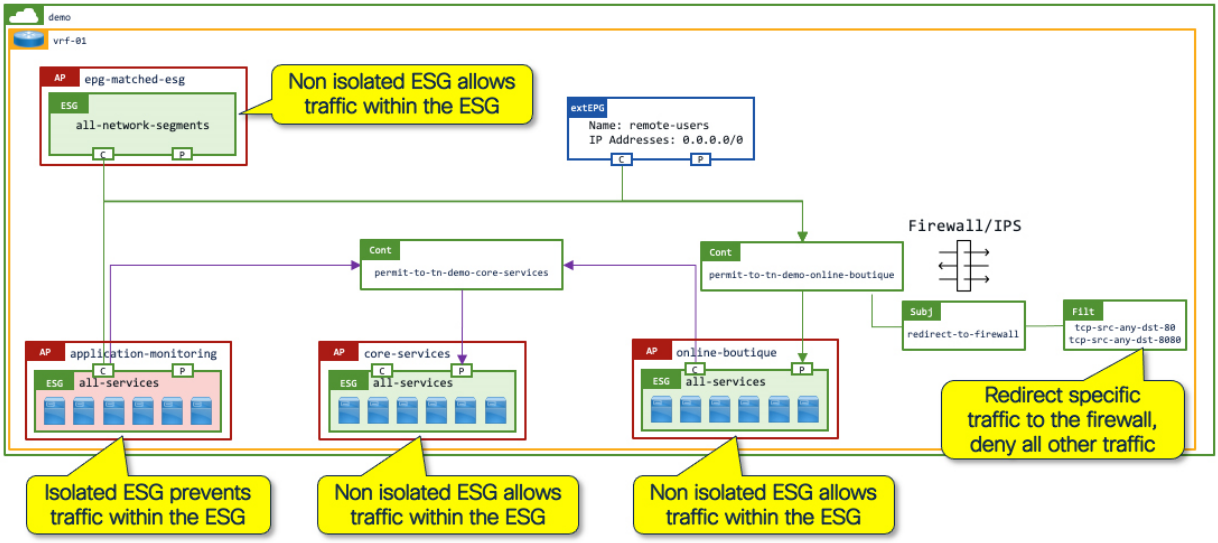


図 24. 疑似企業の Cisco ACI ファブリック：ファイアウォール挿入用の PBR を使用したサービス グラフ

詳細については、ACI 契約ガイド および Cisco ACI ポリシーベース リダイレクトサービス グラフ デザイン ホワイト ペーパー を参照してください。

トラフィックをレイヤ 4 からレイヤ 7 サービス デバイスにリダイレクトするときは、レイヤ 4 からレイヤ 7 サービス デバイスの構成を考慮する必要があります。以下の例では、ESG の柔軟な性質により、異なるサブネットからのエンドポイントを個別のセキュリティ ゾーンに論理的にグループ化できます。ファイアウォールの構成は、ESG から派生した IP アドレス情報を反映する必要があります。これは、ファイアウォール管理プラットフォームが ESG メンバーシップ情報を取得することによって実現できます。

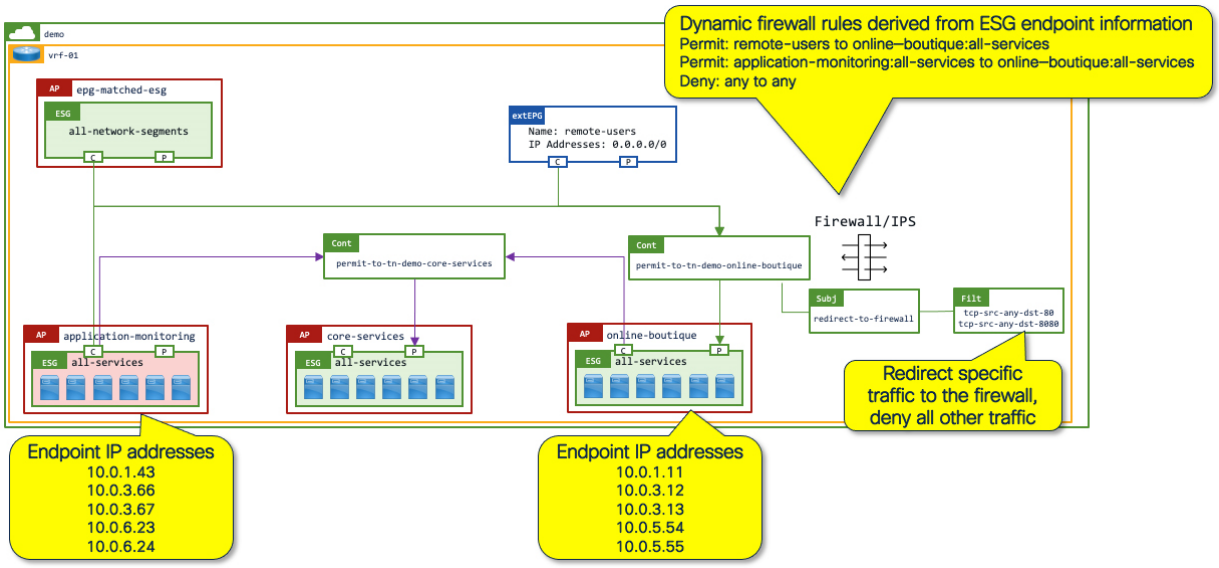


図 25. エンドポイント会員情報

現在、以下のアプリケーションとプラグインが ESG メンバーシップのアドバタイズに利用できます。

- Cisco 適応型セキュリティ アプライアンス（ASA）および Cisco Firepower Threat Defense（FTD）：ACI エンドポイントの更新
- Check Point CloudGuard：ACI 向け CloudGuard
- Fortinet ファブリック コネクタ：Cisco ACI SDN コネクタ
- Palo Alto Networks Panorama：Cisco ACI 用パノラマ プラグイン（ロードマップ）

レイヤ 4 からレイヤ 7 のサービス デバイスが上記のものと異なる場合、エンドポイントから ESG メンバーシップ情報は、Cisco APIC API を使用して取得できます。したがって、単純なスクリプトまたはアプリケーションを使用して情報を取得し、レイヤ 4 からレイヤ 7 のサービス デバイス上に同等のセキュリティ グループを作成できます。詳細については、FAQ を参照します。

ESG デザイン例

この章では、関心のあるユース ケースに直接ジャンプできるように、多くの個別の例を含む ESG のユース ケースを示します（表 2 および表 3）。ESG を初めて使用する場合、またはシナリオ ベースの例のウォークスルーを希望する場合は、ネットワーク セントリックからアプリケーション セントリックへの移行ストーリー：疑似企業。

詳細な設計例のセクションで詳しく説明されているように、ESG は、物理または仮想ワークロードをセグメント化するための多くの柔軟な設計オプションをネットワーク管理者に提供します。きめ細かいアプリケーション中心の ESG を作成するオプションに加えて、Cisco ACI では、ネットワーク管理者が ESG を使用して複数の EP（VLAN）を集約したり、VRF インスタンス内にサブネット ベースのセキュリティ ゾーンを作成したりすることもできます。どちらのオプションも同様に柔軟性があり、同時に使用できます。実際、ESG の強力な利点は、ネットワーク バッキングを変更することなく、エンドポイントをゾーン ベースのセキュリティ環境からアプリケーション ベースのセキュリティ環境にダイナミックに移動できることです。

ESG を備えた柔軟なセキュリティ ゾーン

1. VRF インスタンスごとの単一のセキュリティ ゾーン：VRF インスタンス内のすべての EPG を、すべてのエンドポイントのデフォルトのセキュリティ ゾーンとして単一の ESG にマッピングします。
2. VRF インスタンスごとの複数のセキュリティ ゾーン：EPG のサブセットを ESG セキュリティ ゾーンにマッピングします。VRF インスタンスごとに 1 つ以上の ESG セキュリティ ゾーンを作成します。
3. アプリケーションごとのセキュリティ ゾーン：特定の VRF インスタンス上の任意のサブネットまたは VLAN 全体のタグ セレクタを介して、個々のエンドポイントを ESG にマッピングします。

すべてのエンドポイントが何らかの方法で ESG によってカバーされるように、オプション 1 または 2 を基本構成として使用し、より詳細なセグメンテーション グループにオプション 3 を使用することをお勧めします。次の図は、個別に展開したときの各オプションを示しています。異なるタイプのセレクタを組み合わせるには、FAQ のセレクタの優先順位を参照してください。

次の図は、例 1 で詳しく説明されています。デフォルト ゾーン（EPG セレクタ）としての VRF ごとのセキュリティ ゾーンと図 29。

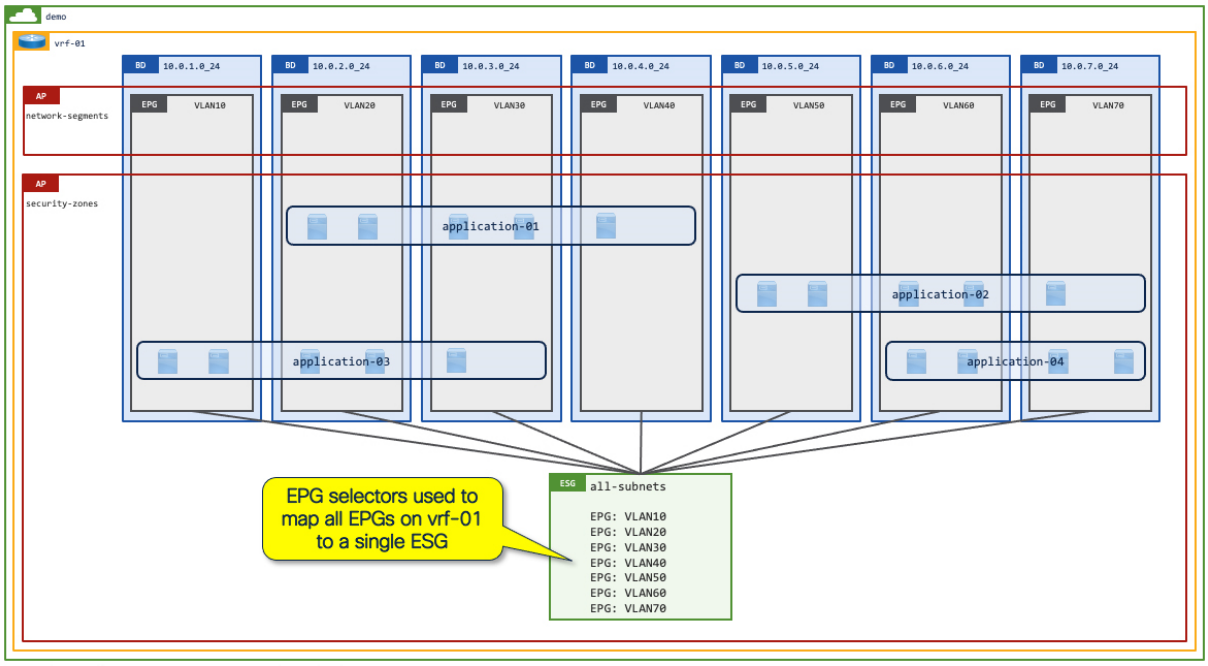


図 26. 同じ VRF インスタンス内のすべてのサブネット / VLAN のデフォルトのセキュリティ ゾーン

次の図は、例 2: サブネット/VLAN（EPG セレクタ）のセットごとのセキュリティ ゾーンと図 30 で詳しく説明されています。

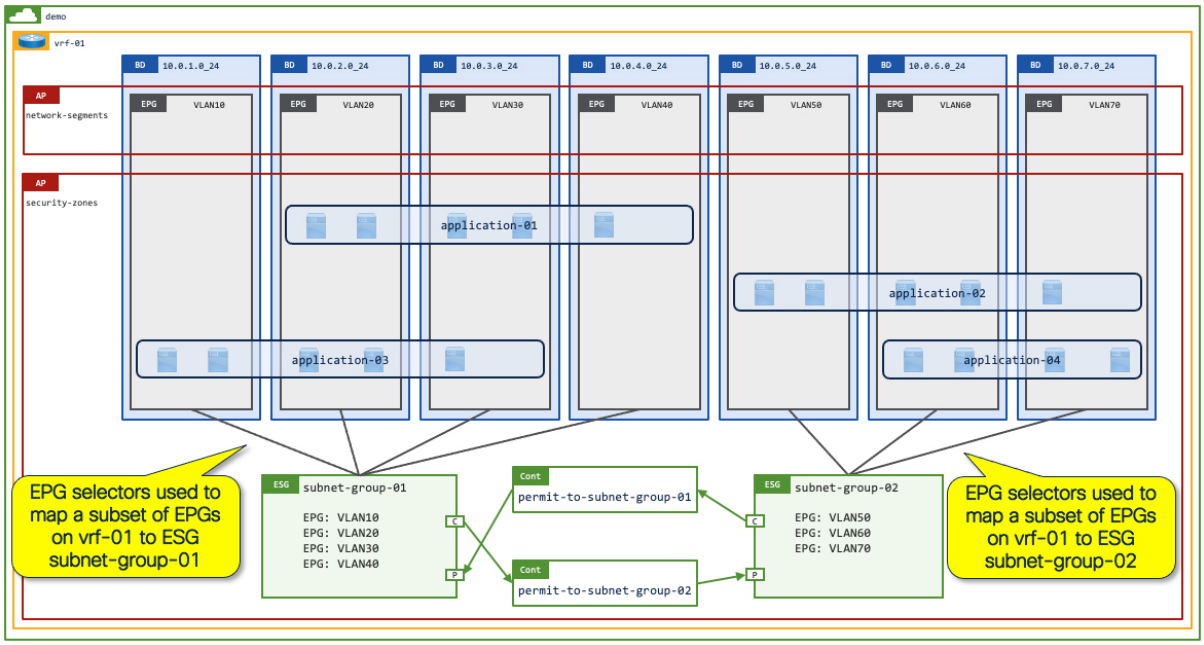


図 27. EPG（サブネット / VLAN）のセットごとのセキュリティ ゾーン

次の図は、VMware vCenter/Cisco APIC タグによって選択されたアプリケーション エンドポイントを示しています。図 31 などの追加の例については、次のセクションで詳しく説明します。

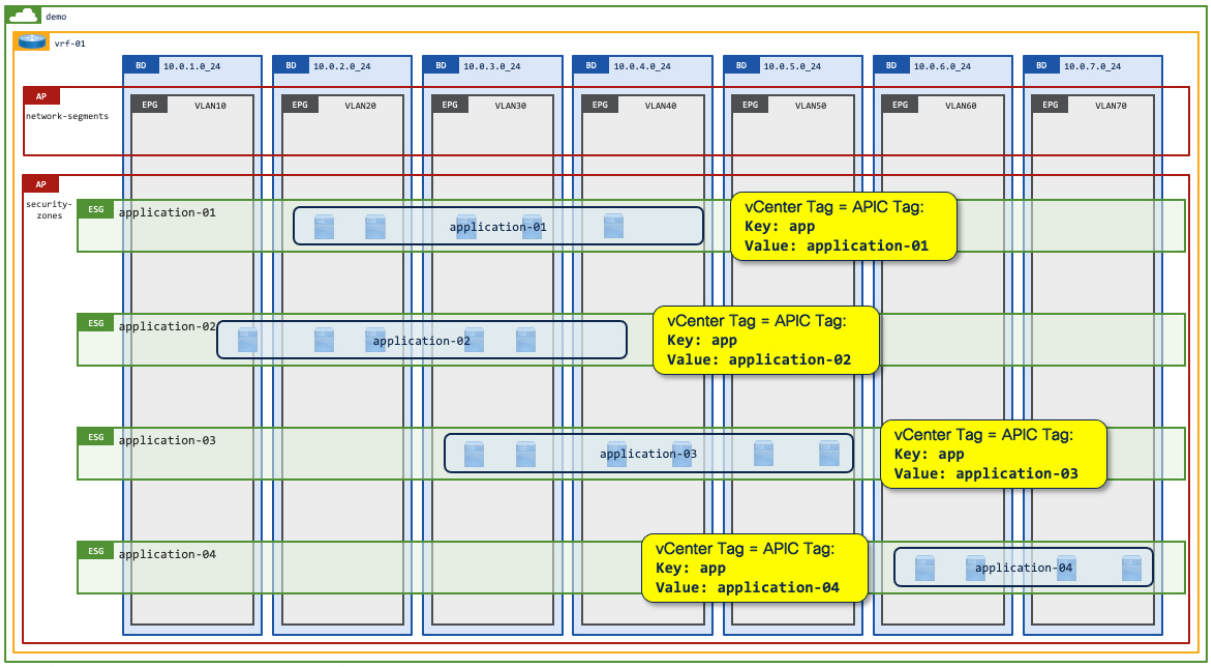


図 28. アプリケーションごとのセキュリティ ゾーン

詳しい設計例

以下の表は、読者がさまざまなセレクタ オプションの使用方法を理解できるように、いくつかの異なる ESG の例をまとめたものです。以下の表に示すように、必要に応じてすべてのオプションを同時に使用できます。

注： ESG 内でレイヤ 2 マルチキャストが必要な場合、セレクタは EPG セレクタまたは MAC アドレスを持つタグ セレクタである必要があります。詳細については、例 12 を参照してください。

表 2 ESG 導入オプションの例 – 単一選択基準

Category	例	説明
EPG セレクタによる基本セキュリティ	例 1：デフォルト ゾーンとしての VRF インスタンスごとのセキュリティ ゾーン （EPG セレクタ）	特定の VRF インスタンスのデフォルト セキュリティ ゾーンとして、すべての EPG を単一の ESG にマッピングします。
	例 2：サブネット/VLAN のセットごとのセキュリティ ゾーン（EPG セレクタ） （VRF インスタンスごとに複数のセキュリティ ゾーン）	EPG のサブセットを ESG セキュリティ ゾーンにマッピングします。VRF インスタンスごとに 1 つ以上の ESG セキュリティ ゾーンを作成します。
タグ セレクタによるきめ細かいセキュリティ	例 3：VMM 統合によるタグ セレクタ	VMware VM タグは、VMM 統合を介して VMware vCenter から取得されます。
サブネットまたは VLAN にまたがる個々のエンドポイントを、VMware タグまたは Cisco APIC ポリシー タグを介して詳細なセキュリティ グループとして ESG にマッピングします。	例 4：MAC アドレスを使用する VM エンドポイントの VMM 統合のないタグ セレクタ	Cisco ACI 管理者は、Cisco APIC 上の各仮想マシン エンドポイントの MAC アドレスに Cisco APIC ポリシー タグを割り当てます。VMware vCenter とのタグ同期はありません。
	例 5：IP アドレスを使用する VM エンドポイントの VMM 統合なしのタグ セレクタ	Cisco ACI 管理者は、Cisco APIC 上の各仮想マシン エンドポイントの IP アドレスに Cisco APIC ポリシー タグを割り当てます。VMware vCenter とのタグ同期はありません。
	例 6：MAC アドレスを使用したベア メタル エンドポイントのタグ セレクタ	Cisco ACI 管理者は、Cisco APIC の各ベア メタル エンドポイントの MAC アドレスに Cisco APIC ポリシー タグを割り当てます。
	例 7：IP アドレスを使用したベア メタル エンドポイントのタグ セレクタ	Cisco ACI 管理者は、Cisco APIC の各ベア メタル エンドポイントの IP アドレスに Cisco APIC ポリシー タグを割り当てます。
	例 8：中間スイッチを備えたタグ セレクタ	Cisco 以外の中間スイッチには PVLAN が必要です。
IP サブネット セレクタによるきめ細かいセキュリティ	例 9：IP サブネット セレクタ	IP アドレスまたはサブネットを ESG に直接割り当てます。

次の表は、複数のセレクタを組み合わせて使用する追加の例を示しています。

表 3 ESG 展開オプションの例 – 複数の選択基準

例	説明
例 10：EPG セレクタを介したデフォルトのセキュリティ ゾーンを持つタグ セレクタを介したアプリケーション エンドポイントのコンテナとしての ESG。	ネットワーク セントリックからアプリケーション セントリックへの移行ストーリーの章の例: 疑似企業。
例 11：タグ セレクタを介した検疫 ESG を持つ EPG セレクタを介した複数のセキュリティ ゾーン。	誤動作または脆弱なエンドポイントにタグを割り当てて、各セキュリティ ゾーンから隔離します。
例 12：レイヤ 2 マルチキャストを使用した ESG。	L2 マルチキャスト / フラッド トラフィックがある状況での ESG の設計方法の例。

例 13：EPG セレクタと IP ベースのセレクタ	EPG が EPG セレクタを使用して ESG に一致する場合に、IP ベースのセレクタのプロキシ ARP を構成する方法の例。

例 1：デフォルト ゾーンとしての VRF インスタンスごとのセキュリティ ゾーン（EPG セレクタ）

多くのお客様は、vzAny で提供および使用されるすべての許可契約を使用して Cisco ACI 展開を開始するか、代わりに優先グループにすべての EPG を含めて、VRF インスタンス内のすべての通信を許可し、後でより多くのセキュリティを徐々に実装することを目的としています。ESG は、ネットワーク管理者が、将来に向けてより優れた拡張性を備えたシンプルで柔軟な開始点を持てるようにすることで、このアプローチを簡素化できます。EPG セレクタを使用して VRF インスタンス内のすべての EPG を単一の ESG にマッピングすることにより、ESG はデフォルトのセキュリティ ゾーンとして機能します。この基本セキュリティ ゾーンを作成したら、他のより詳細な ESG に分類するエンドポイントを明示的に選択できます。

デフォルトのセキュリティ ゾーンとしての ESG は、VRF インスタンス内のすべての EPG を EPG セレクターを使用して ESG にマッピングすることにより、VRF インスタンス内のすべてのエンドポイントのフォールバックとして機能します。以下に示すすべてのエンドポイントは、同じ ESG に属しているため、相互に通信できます。ネットワーク管理者は、（デフォルトで）すべての ESG 内トラフィックがファイアウォールにリダイレクトされるように、サービス グラフ PBR を使用して ESG 内契約を実装できます。または、デフォルトのセキュリティ ゾーン ESG を構成して分離を適用し、ワークロードが関連する契約を使用して適切なアプリケーション ESG に移動するまで、ESG 内通信を防止することもできます。

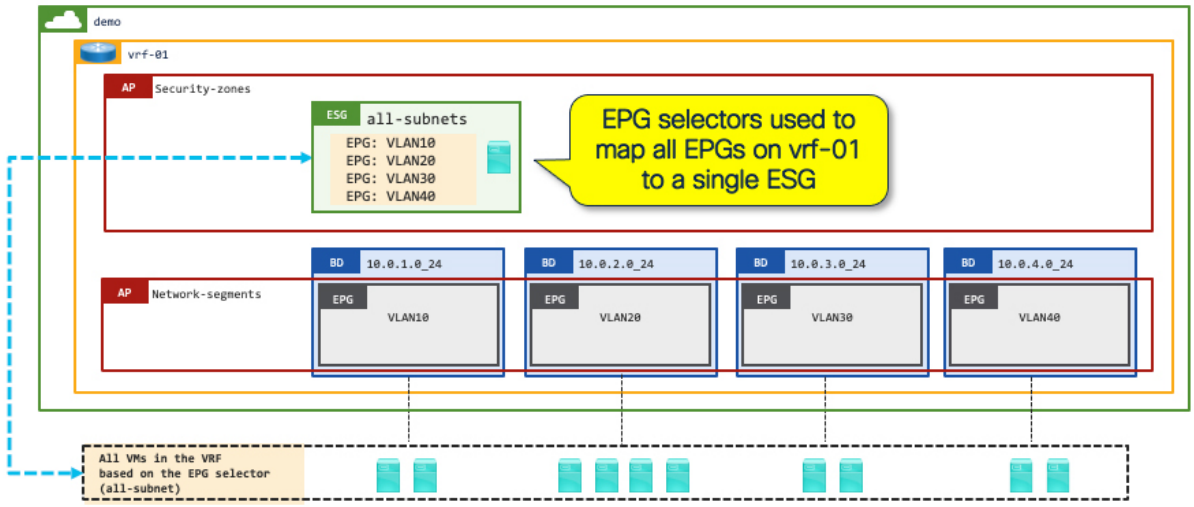


図 29. 設計例：特定の VRF インスタンスのデフォルト セキュリティ ゾーン

例 2：サブネット/ VLAN のセットごとのセキュリティ ゾーン（EPG セレクタ）

前の例に示したように、特定の VRF インスタンスに対して単一のデフォルト セキュリティ ゾーンを作成する代わりに、EPG セレクタを備えた ESG は、各ゾーンが 1 つのブリッジ ドメインに制限されることなく、同じ VRF インスタンス内に複数のセキュリティ ゾーンを簡単に作成できます。このユース ケースでは、各 ESG は、組織のセキュリティ要件に基づいて、組織や開発グループなどの 1 つのエンクレーブを表します。これにより、追加の構成なしで各エンクレーブ内での通信が可能になりますが、デフォルトでは、エンクレーブ間の通信がブロックされます。各エンクレーブには、ブリッジ ドメイン全体のエンドポイントのセットで構成される複数のアプリケーションが含まれている可能性があります。エンドポイントは複数のブリッジ ドメインにまたがって配置されるため、EPG を使用してこの設計を実現することはできません。

この例では、各エンクレーブに一連の専用 VLAN / サブネットが割り当てられています。たとえば、ESG サブネット グループ-01 の VLAN 10 と 20、ESG サブネット グループ-02 の VLAN 30 と 40 です。この状況では、ネットワーク管理者は EPG セレクタを使用して、エンクレーブごとに ESG を簡単に作成できます。

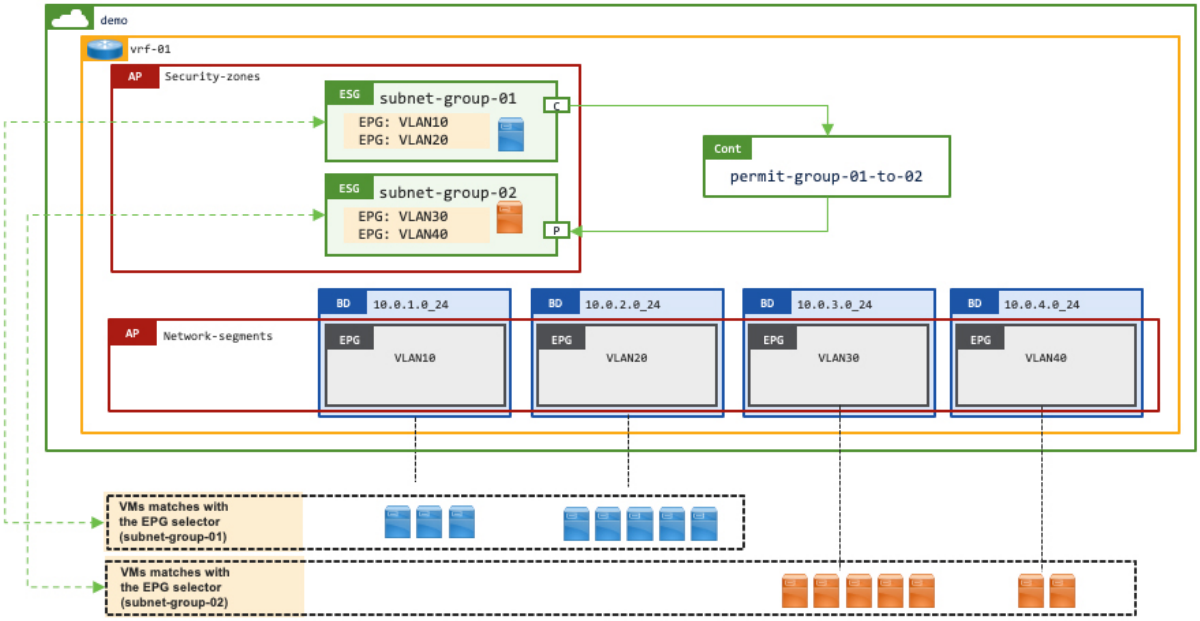


図 30. 設計例：特定の VRF インスタンスの複数のデフォルト セキュリティ ゾーン

例 3：VMM 統合によるタグ セレクタ

これは、VMware vCenter からの VM タグまたは VM 名に一致する ESG タグ セレクターの例です。このユースケースでは、読み取り専用ではなく、読み取り / 書き込みアクセス許可を備えた VMM ドメイン統合が必要です。読み取り専用統合を備えた Cisco APIC は VM 名とタグを VMware vCenter から取得しますが、そのようなデータは EPG や ESG などのテナント オブジェクトに関連付けられません。したがって、現在これらを ESG セレクタに利用することはできません。

タグ セレクタに VM タグまたは VM 名を使用する場合、タグ セレクタ自体に加えて、次の 2 つの構成が必要です。

- VMM ドメイン自体で「タグ コレクション」を有効にします。
- EPG の VMM ドメイン アソシエーションを介して「マイクロ セグメンテーションを許可する」を有効にします。
  - これにより、Cisco ACI リーフ スイッチと VMware vCenter ポート グループに PVLAN が自動的に展開されます。これは、VMware 仮想スイッチがトラフィックを Cisco ACI に転送せずに同じポート グループ内のトラフィックをブリッジするのを防ぐためです。

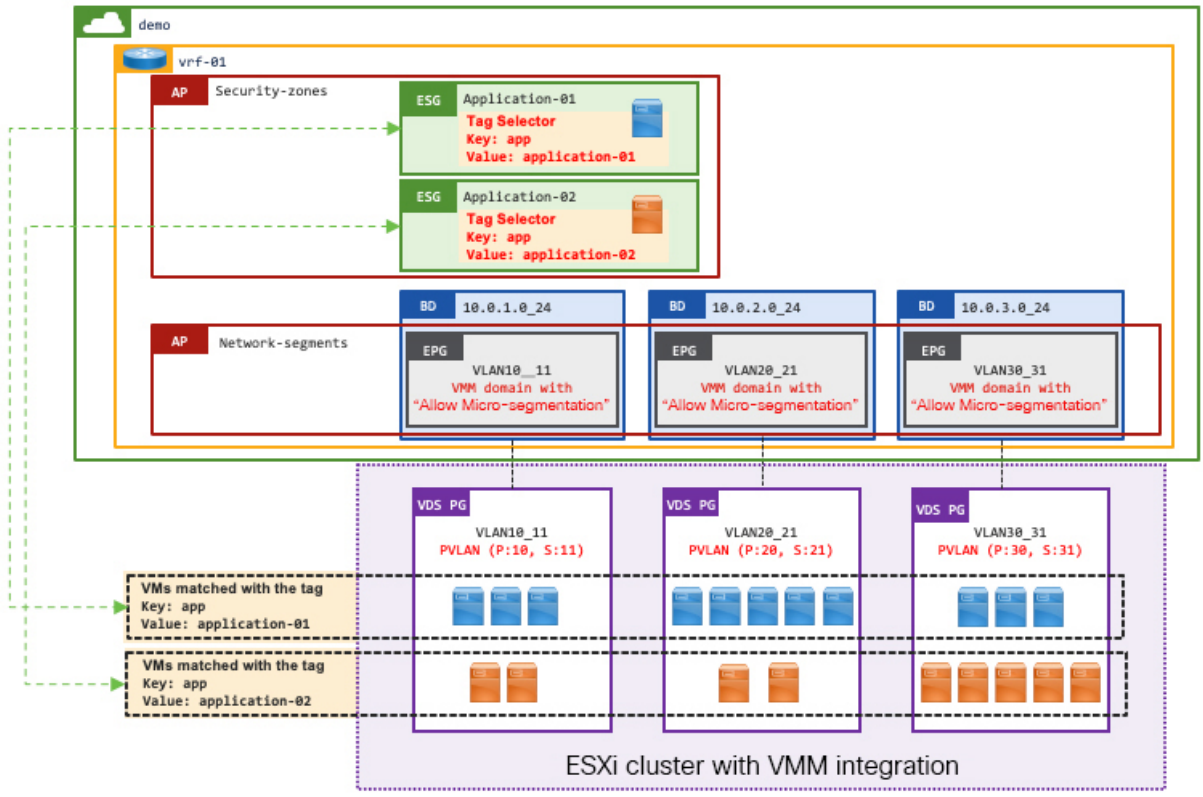


図 31. 設計例：VMM 統合によるタグ セレクタ

例 4：MAC アドレスを使用する VM エンドポイントの VMM 統合のないタグ セレクタ

この例は、MAC アドレスを使用して VM エンドポイントと一致する ESG タグ セレクタを示しています。このオプションは、読み書き VMM 統合のない ESX クラスタを使用しているお客様に適用されます。

vCenter VMM 統合なしで、「物理」ドメインを介して、VMware vCenter 上の VM エンドポイントを Cisco ACI ファブリックに接続できます。VMware vCenter に物理ドメインを使用している場合は、オプションで、読み取り専用の VMM を統合して、Cisco APIC が VM エンドポイントの接続の可視性を取得できるようにすることができます。ただし、読み書き VMM 統合なしでは、ESG 分類のために VMware vCenter で VM タグまたは VM 名を使用することはできません。

次の例では、タグ セレクタ自体の上に次の 3 つの構成オプションが必要です。

- Cisco APIC の各 MAC アドレスに Cisco APIC ポリシー タグを手動で作成して割り当てます。
- VMware vCenter の Cisco ACI EPG（VLAN）とポート グループの両方で PVLAN を手動で構成します。
  - これにより、VMware 仮想スイッチがトラフィックを Cisco ACI に転送せずに同じポート グループ内のトラフィックをブリッジできなくなります。
- （オプション）EPG でプロキシ ARP を有効にします。
  - PVLAN が有効になっている場合、フラッディングまたはレイヤ 2 マルチキャスト トラフィックは、各 EPG 内および PVLAN を使用する EPG 間でブロックされます。これにより、それらの EPG のエンドポイント間で ARP が解決されなくなり、プロキシ ARP は、ターゲット エンドポイントに代わって ARP 要求に応答する Cisco ACI リーフ スイッチによってこの制限を解決します。デフォルト ゲートウェイである必

要がある Cisco ACI ブリッジ ドメイン SVI への ARP 要求は PVLAN によってブロックされないため、異なるサブネット内のエンドポイント間の通信にはプロキシ ARP は必要ないことに注意してください。

静的ポート（静的パス バインディング）を使用して、物理ドメインを持つ Cisco ACI EPG で PVLAN を手動で設定します。Cisco ACI EPG の PVLAN には、次のいずれかの構成も必要です：

- EPG 内で分離を有効にします
- EPG 内契約の構成

次のオプションとともにプロキシ ARP を有効にすることもできます。

- Intra-EPG 分離を有効にしてから、プロキシ ARP を明示的に有効にします。
- Intra-EPG コントラクトを構成すると、プロキシ ARP が暗黙的に有効になります

この例では、最初のオプション（プロキシ ARP を使用した Intra-EPG 分離）が使用されます。

注：　統合プロセスを合理化するために、ネットワーク管理者は、Ansible、Terraform、または python などの自動化ツールを使用して、VMware vCenter から仮想マシンの MAC アドレスを読み取り、Cisco APIC で MAC タグを作成できます。自動化を使用して、Cisco APIC での EPG/VLAN 静的バインディングと、VMware vCenter での PVLAN ポート グループの両方を作成することもできます。

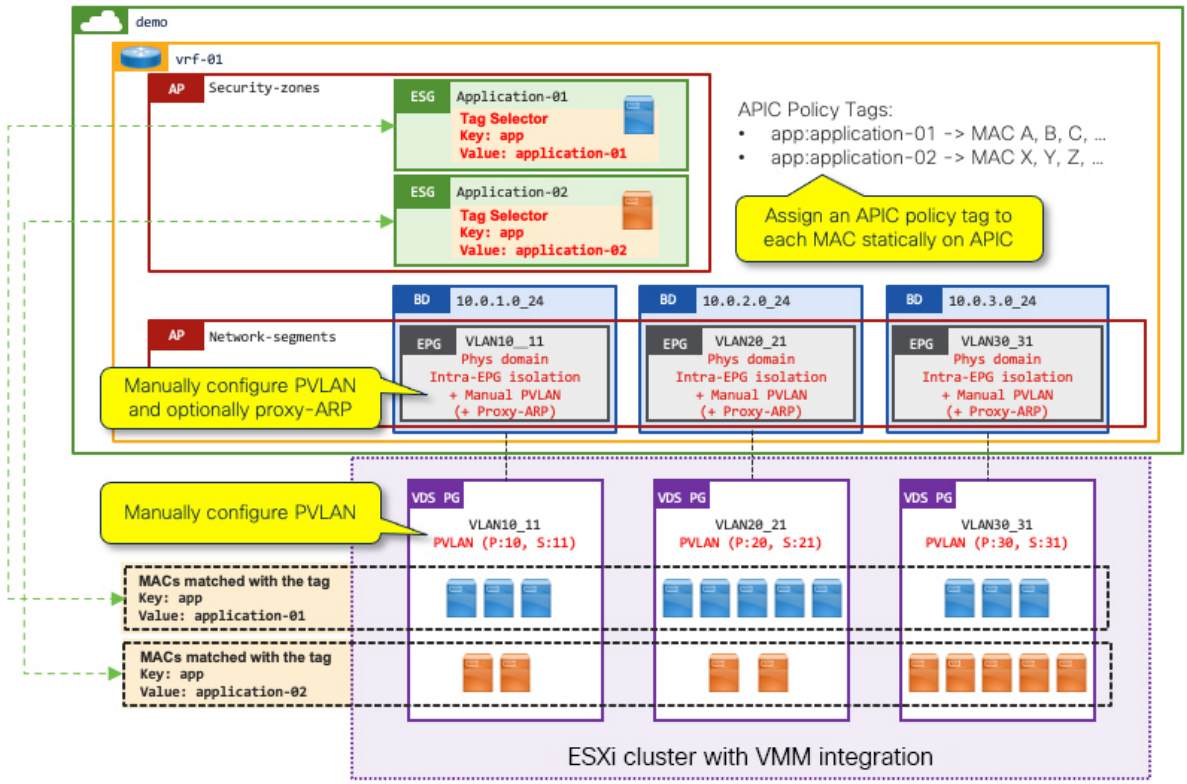


図 32.　設計例：MAC アドレスを使用する VM エンドポイントの VMM 統合のないタグ セレクタ

例 5：IP アドレスを使用する VM エンドポイントの VMM 統合なしのタグ セレクタ

この例は、IP アドレスを介して VM エンドポイントに一致する ESG タグ セレクタを示しています。このオプションは、読み取り / 書き込み VMM 統合のない ESX クラスタを使用しているお客様に適用されます。

VMware vCenter 上の VM エンドポイントは、vCenter VMM 統合なしで「物理」ドメインを介して Cisco ACI ファブリックに接続できます。VMware vCenter の物理ドメインを使用しているお客様は、オプションで読み取り専用の VMM 統合を使用して、Cisco APIC が VM エンドポイントの接続を表示できるようにすることができます。ただし、VMware vCenter 上の VM タグまたは VM 名は、読み書き VMM 統合なしでは ESG 分類に使用できません。

この例では、タグ セレクタに加えて、次の 3 つの構成オプションが必要です。

- Cisco APIC の各 IP アドレスに Cisco APIC ポリシー タグを手動で作成して割り当てます。
- VMware vCenter の Cisco ACI EPG（VLAN）とポート グループの両方で PVLAN を手動で構成します。
  - これは、VMware 仮想スイッチがトラフィックを Cisco ACI に転送せずに同じポート グループ内のトラフィックをブリッジするのを防ぐためです。
- EPG でプロキシ ARP を有効にします。
  - Cisco ACI スイッチが IP アドレスに基づいて ESG セキュリティを適用するには、トラフィックをブリッジではなくルーティングする必要があります。すべてのトラフィックがルーティングされたトラフィックとして処理されるようにするには、EPG でプロキシ ARP を有効にする必要があります。
  - PVLAN が有効になっている場合、フラッディングまたはレイヤ 2 マルチキャスト トラフィックは、各 EPG 内および PVLAN を使用する EPG 間でブロックされます。これにより、それらの EPG のエンドポイント間で ARP が解決されなくなり、プロキシ ARP は、ターゲット エンドポイントに代わって ARP 要求に応答する Cisco ACI リーフ スイッチによってこの制限を解決します。

この例は、最初のポイント（MAC アドレスではなく IP アドレス）と 3 番目のポイント（プロキシ ARP が必須）を除いて、例 4：MAC アドレスを介した VM エンドポイントの VMM 統合なしのタグ セレクタと非常に似ています。

静的ポート（静的パス バインディング）を使用して、物理ドメインを持つ Cisco ACI EPG で PVLAN を手動で設定します。Cisco ACI EPG の PVLAN には、次のいずれかの構成も必要です：

- EPG 内で分離を有効にします
- EPG 内契約の構成

プロキシ ARP は、次のオプションとともに有効にすることもできます。

- EPG 内分離を有効にしてから、プロキシ ARP を明示的に有効にする
- EPG 内コントラクトを構成すると、プロキシ ARP が暗黙的に有効になります

この例では、最初のオプション（EPG 内分離とプロキシ ARP）を使用します。

注：　統合プロセスを合理化するために、ネットワーク管理者は、Ansible、Terraform、または python などの自動化ツールを使用して、VMware vCenter から仮想マシンの IP アドレスを読み取り、Cisco APIC で IP タグを作成できます。自動化を使用して、Cisco APIC の EPG / VLAN 静的バインディングと VMware vCenter の PVLAN ポート グループの両方を作成することもできます。

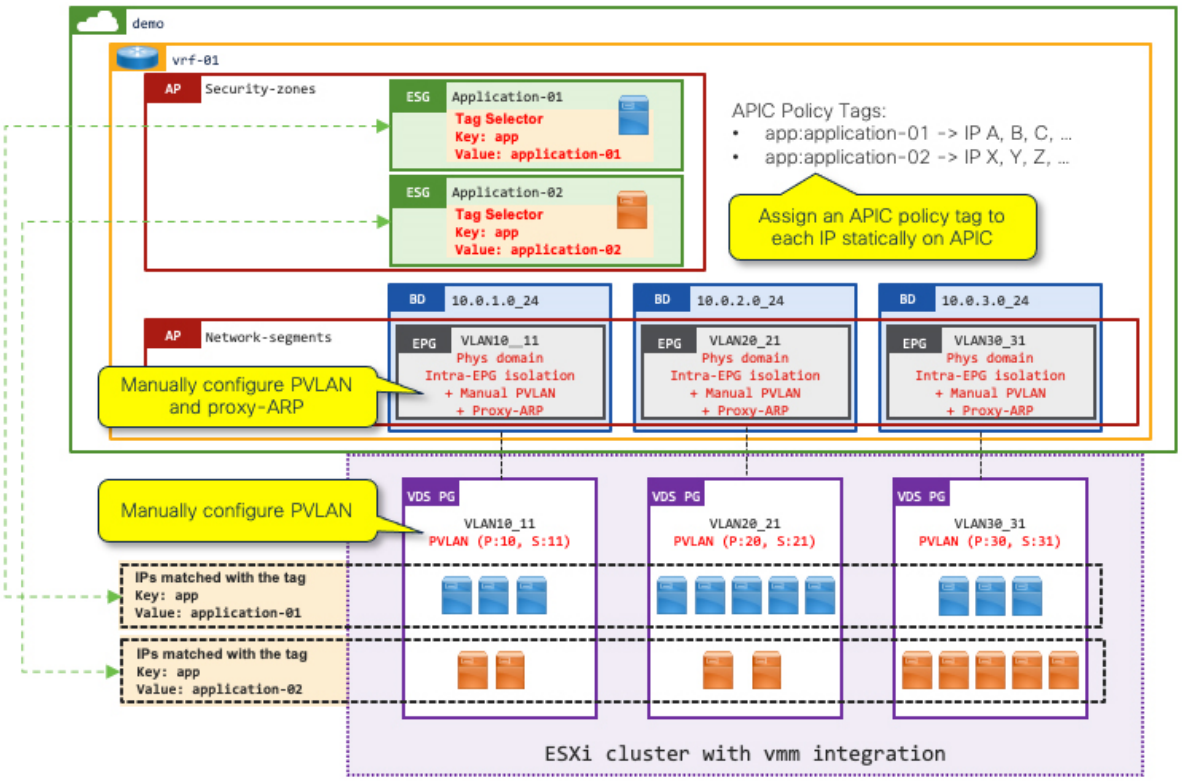


図 33. 設計例：IP アドレスを使用する VM エンドポイントの VMM 統合のないタグ セレクタ

例 6：MAC アドレスを使用したベア メタル エンドポイントのタグ セレクタ

この例は、各エンドポイントの MAC アドレスに静的にアタッチされた Cisco ACI ポリシー タグを介してベア メタル エンドポイントに一致する ESG タグ セレクタを示しています。

これは、vDS を構成しないことを除いて、例 4：MAC アドレスを介した VM エンドポイントの VMM 統合を使用しないタグ セレクタと同じです。ブレードや仮想スイッチなどの中間スイッチがないため、EPG での PVLAN 構成も必要ありません。エンドポイントと Cisco ACI スイッチの間に Cisco 以外の ACI スイッチがある場合でも、PVLAN は必要です。ユース ケースの例については、例 8：中間スイッチを備えたタグ セレクタを参照してください。

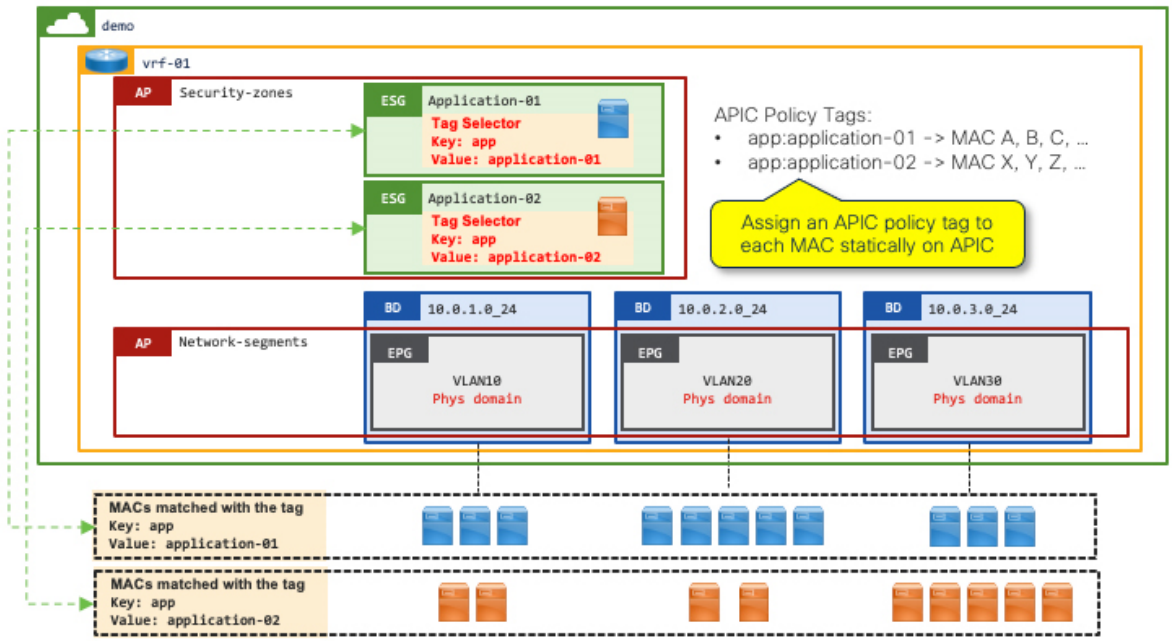


図 34. 設計例：MAC アドレスを使用したベア メタル エンドポイントのタグ セレクタ

例 7：IP アドレスを使用したベア メタル エンドポイントのタグ セレクタ

この例は、各エンドポイントの IP アドレスにアタッチされた Cisco ACI ポリシー タグを介してベア メタル エンドポイントに一致する ESG タグ セレクタを示しています。

これは、vDS を構成しないことを除いて、例 5：「IP アドレスを介した VM エンドポイントの VMM 統合のないタグ セレクタ」と同じです。ブレード スイッチなどの中間スイッチがないため、EPG での PVLAN 構成も必要ありません。エンドポイントと Cisco ACI スイッチの間に Cisco 以外の ACI スイッチがある場合でも、PVLAN は必要です。ユース ケースの例については、例 8：「中間スイッチを備えたタグ セレクタ」を参照してください。

注：　この例では選択基準として IP アドレスを使用しているため、プロキシ ARP は引き続き必要です。

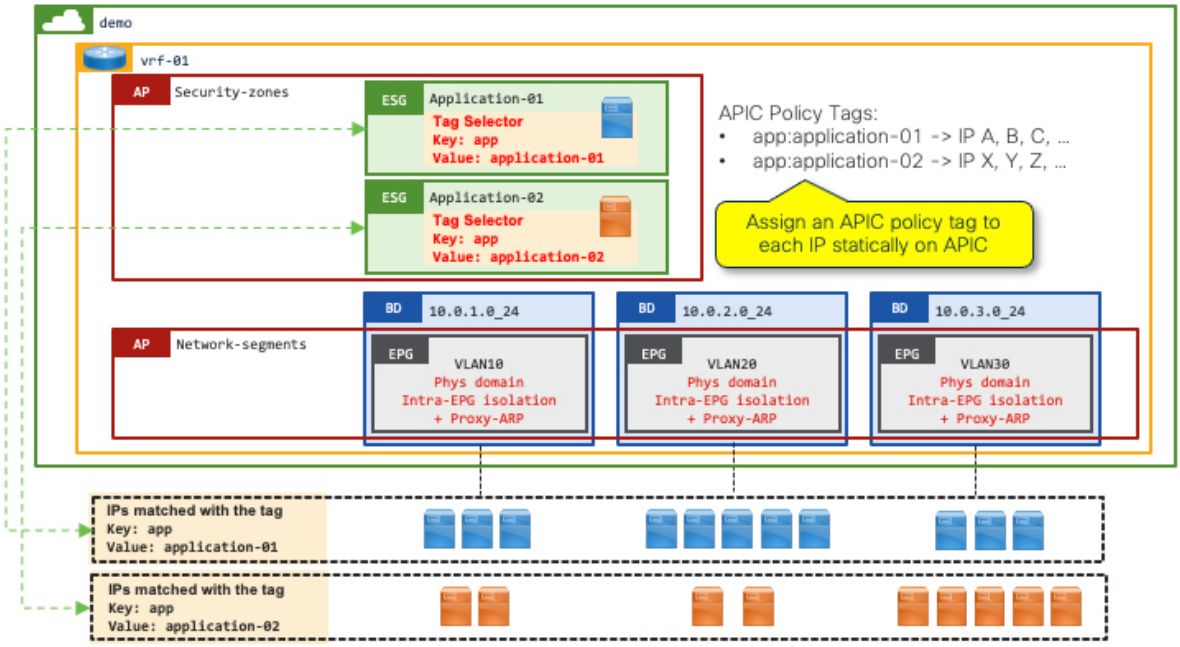


図 35. 設計例：IP アドレスを使用したベア メタル エンドポイントのタグ セレクタ

例 8：中間スイッチを備えたタグ セレクタ

これは、Cisco ACI リーフ スイッチとエンドポイントの間に中間スイッチがある例です。VM エンドポイントの場合、それらは Cisco UCS ファブリック インターコネクトなどのブレード スイッチまたは仮想化ソリューションの仮想スイッチの背後にある可能性があります。

このような場合、PVLAN を Cisco ACI リーフ スイッチから中間スイッチを介して仮想スイッチの vDS ポート グループに拡張する必要があります。これは、これらのスイッチが、ESG セキュリティが適用されている Cisco ACI リーフ スイッチに到達する前に、VLAN に基づいてトラフィックをブリッジしないようにするためです。

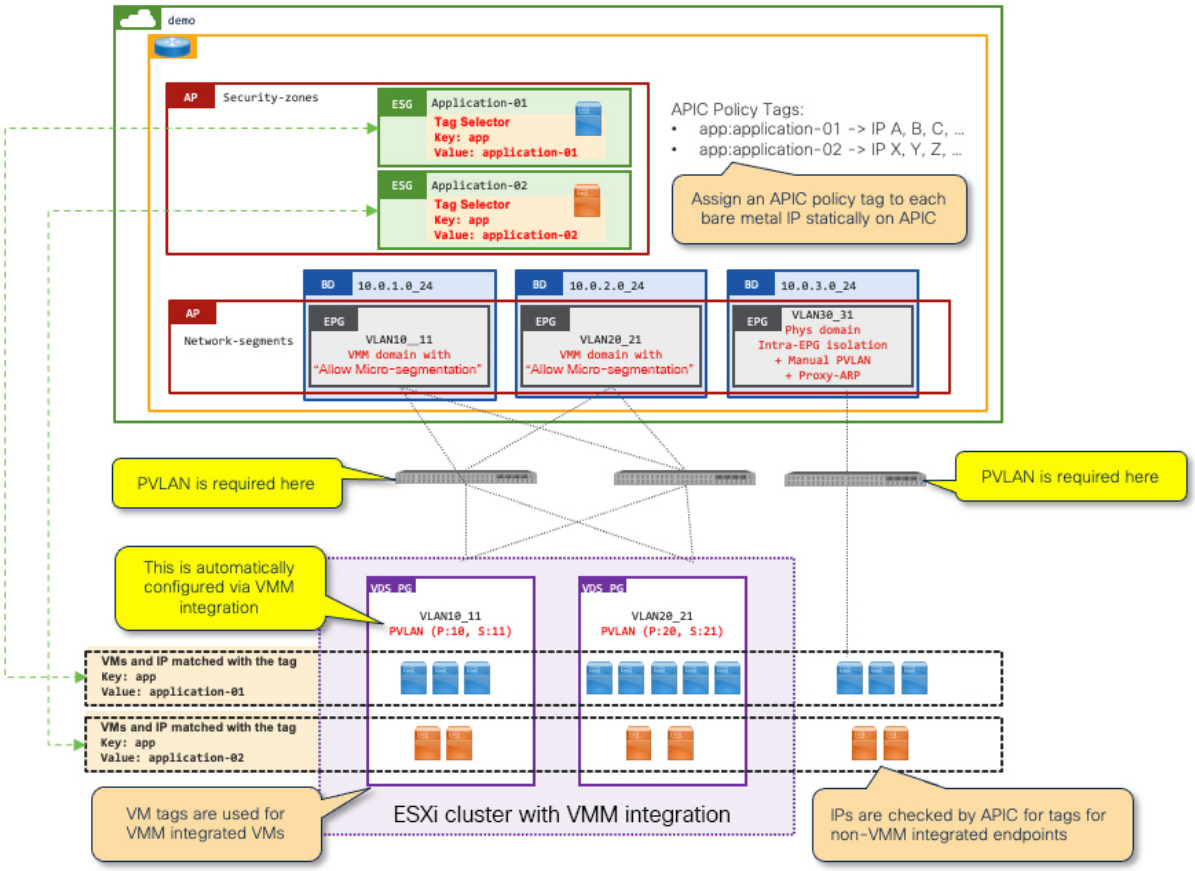


図 36. 設計例：中間スイッチを備えたタグ セレクタ

例 9：IP サブネット セレクタ

これは、タグなしで ESG 直下の IP アドレスまたはサブネットを指定する方法の例です。これは、特定の範囲内のすべての IP アドレスが同じ ESG に属する必要がある場合に役立ちます。

これは基準として IP アドレスを使用するため、他の IP アドレスの例で説明されているプロキシ ARP 要件もここで適用できます。そのため、ブリッジ ドメイン サブネットまたは複数のブリッジ ドメイン サブネット内のすべてのエンドポイントが同じ ESG に属する必要がある場合は、代わりに EPG セレクタを使用してブリッジ ドメイン内のすべての EPG と一致させることをお勧めします。ただし、EPG と ESG が異なるテナントに属している場合（たとえば、ESG がユーザー テナントに属しているときに EPG がテナント ***共通*** に属している場合）、EPG セレクターはサポートされません。このような場合でも、IP サブネット セレクタを使用できます。

この例では、エンドポイントが VMM 統合かベアメタルかに関係なく、IP サブネット セレクタを使用して、各ブリッジ ドメイン サブネットの半分を 1 つの ESG に分類し、残りの半分を別の ESG に分類します。VM エンドポイントの場合、中間仮想スイッチのため、ポート グループに PVLAN が必要です。この例では、VMM 統合で「マイクロセグメンテーションを許可」オプションを使用して、これを実現しています。「マイクロ セグメンテーションを許可」も暗黙的にプロキシ ARP を有効にします。

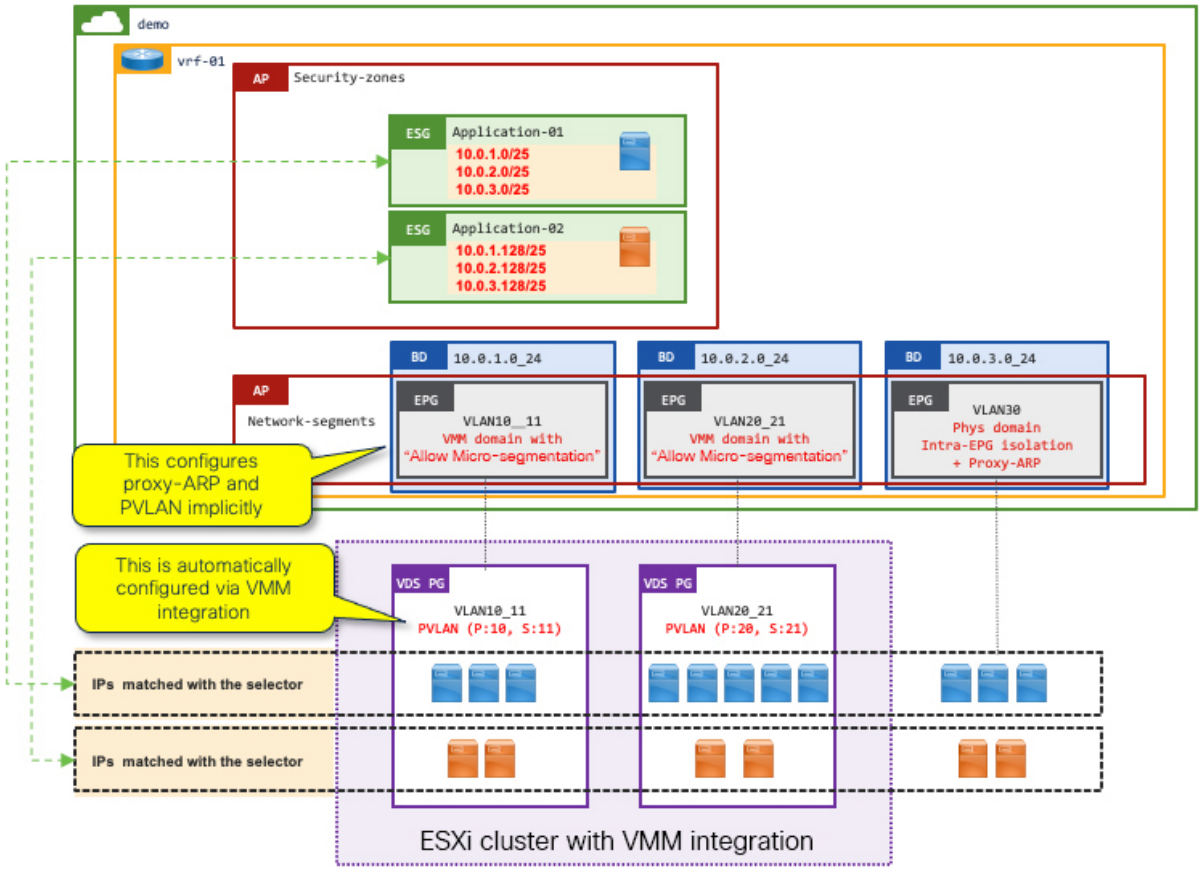


図 37. 設計例：IP サブネット セレクタ

例 10：EPG セレクタを使用するデフォルトのセキュリティ ゾーンを持つタグ セレクターを使用するアプリケーションのコンテナーとしての ESG

次の例では、さまざまなタイプのセレクタを一緒に使用しています。

- **VRF インスタンスごとのセキュリティ ゾーン（EPG セレクタ）**– デフォルトではエンドポイントが相互に通信できないように、ESG 内で分離されたキャッチオール グループとしての VRF インスタンスのデフォルトのセキュリティ ゾーン
- **アプリケーションごとのセキュリティ ゾーン（VMM 統合を備えたタグ セレクタ）**- 既定のセキュリティ ゾーンからエンドポイントをプルして、同じグループまたはコントラクトを使用して別のグループの他のグループと通信できるようにします。

これは、Network Centric to Application Centric Migration Story：疑似企業の章の例に相当します。

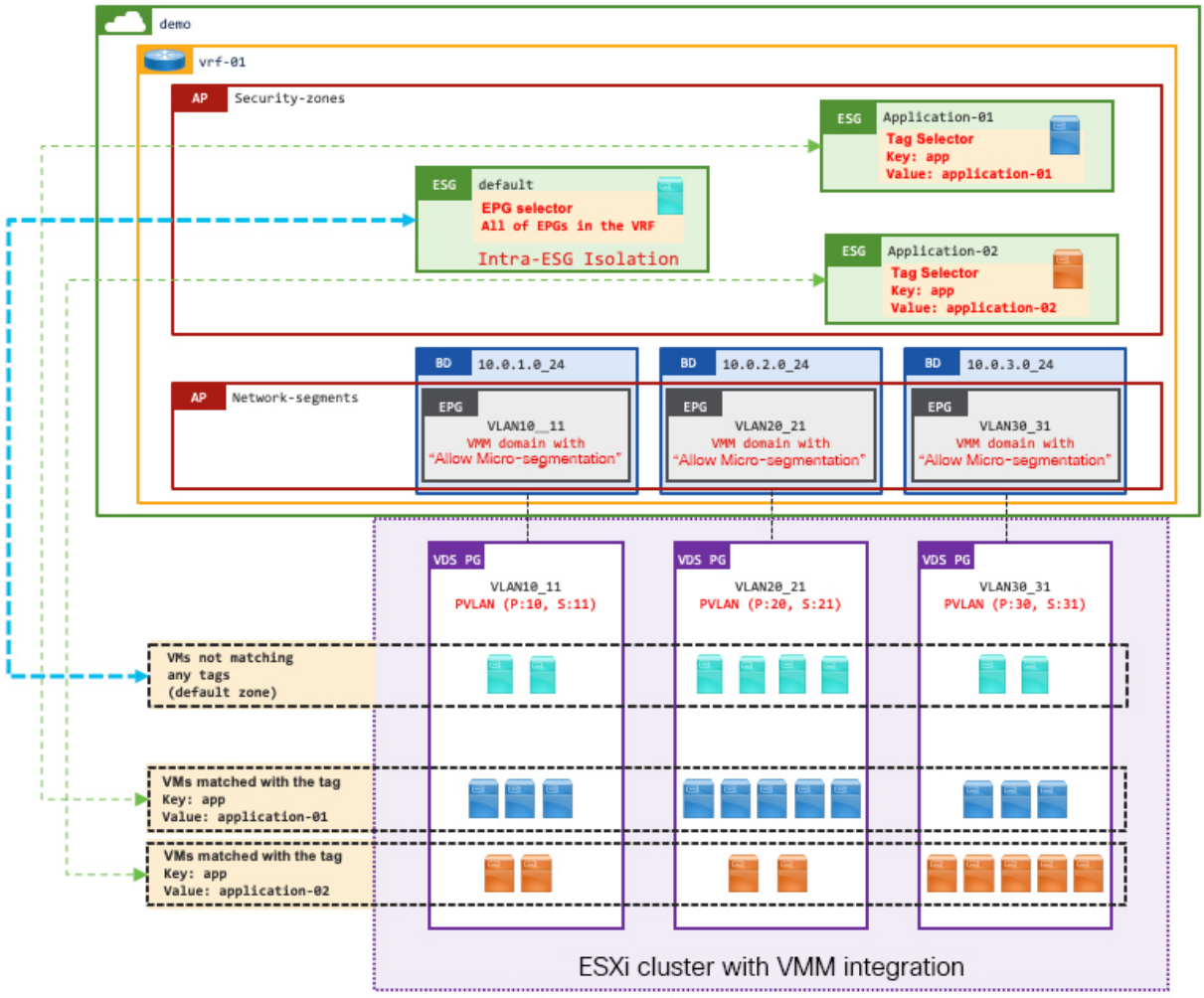


図 38. 設計例：アプリケーションごとの ESG のタグ セレクタおよびデフォルトのセキュリティ ゾーンの EPG セレクタ

例 11：タグ セレクターを使用する検疫 ESG で EPG セレクタを使用する複数のセキュリティ ゾーン。
次の例では、さまざまなタイプのセレクタを一緒に使用しています。

- **サブネット / VLAN（EPG セレクタ）ごとのセキュリティ ゾーン – EPG によって表されるサブネットまたは VLAN のセットで構成されるエンクレーブごとの基本セキュリティ ゾーンとして。**各ゾーン（ESG）のエンドポイントは、デフォルトで相互に通信できます。各ゾーン間の通信は、コントラクトを使用して明示的に許可されます。
- **検疫セキュリティ ゾーン（VMM 統合を備えたタグ セレクタ） - 悪意のあるエンドポイントを各セキュリティ ゾーンからプルして検疫するため。**検疫ゾーンは、ゾーン（ESG）内のすべてのトラフィックをブロックするために、ESG 内分離で構成されます。

これは、例 10：EPG セレクタを介したデフォルトのセキュリティ ゾーンを持つタグ セレクタを介したアプリケーションのコンテナとしての ESG と同じセレクタ（EPG およびタグ）のセットを使用していますが、逆の方法で使用します。この例では、デフォルトで、エンドポイントはネットワーク分散（サブネット / VLAN）に基づいた適切なセキュリティ設定を持つそれぞれのセキュリティ ゾーン（ESG）に属し、タグは特定のエンドポイントからの通信を許可するセキュリティ ポリシーを取り消すために使用されます。

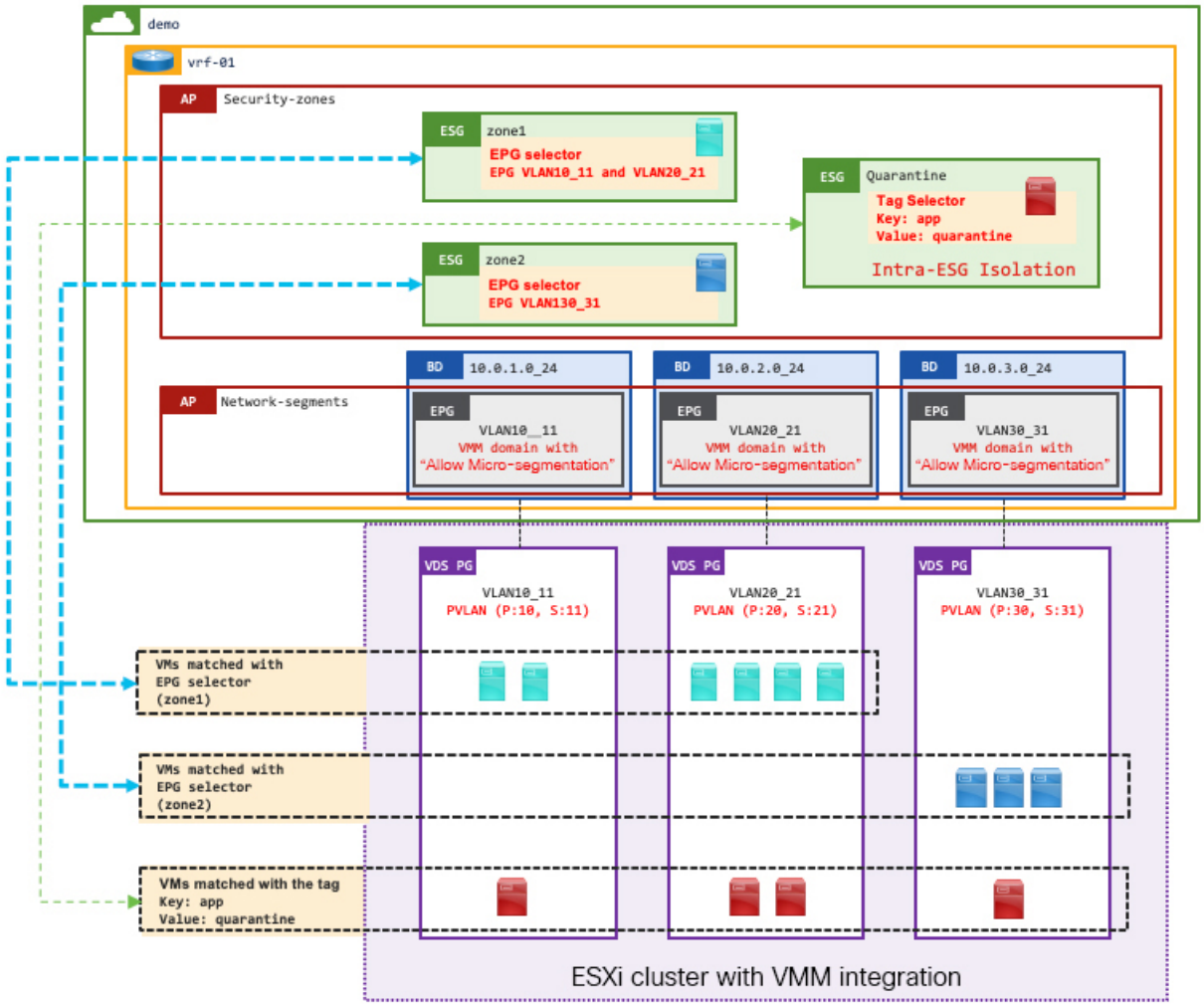


図 39. タグ セレクタを使用する隔離 ESG を備えた EPG セレクタを使用する複数のセキュリティ ゾーン。

例 12：レイヤ 2 マルチキャストを使用した ESG。

クラスタ キープアライブやマルチキャスト DNS など、ESG 内のエンドポイント通信にレイヤー 2 マルチキャストが必要な場合、以下に示す構成オプションは要件に干渉します。これらのオプションはフラッディングとレイヤ 2 マルチキャスト トラフィックをブロックするためです。

- EPG 内分離
- 内通 EPG 契約
- VMM ドメインで「マイクロセグメンテーションを許可する」

注： Intra-EPG 分離 / 契約は、EPG 間およびこれらの設定を持つ EPG 内のフラッディングとレイヤ 2 マルチキャスト トラフィックをブロックします。ただし、「マイクロセグメンテーションを許可する」を使用すると、影響の範囲は EPG 全体ではなく VLAN になります。

つまり、これらの構成を必要とするセレクタは、そのような状況では使用できません。

レイヤ 2 マルチキャストに使用できるセレクタ、つまり、上記の構成を必要としないセレクタは次のとおりです。

- EPG セレクタ
- MAC アドレスを持つタグ セレクタ

以下、各セレクタの詳細について説明します。

EPG セレクタ
これらのセレクタは、レイヤ 2 マルチキャスト転送を妨げる上記の構成オプションを必要としません。

例 1 または 例 2 を参照してください。

MAC アドレスを持つタグ セレクタ
これらのセレクタは、PVLAN が必要ない場合、レイヤ 2 マルチキャストの要件を満たすことができます。つまり、リーフ スイッチとエンドポイントの間に中間スイッチがない場合です。

例 6 : MAC アドレス経由のベア メタル エンドポイントのタグ セレクタを参照してください。

VM タグまたは VM 名を持つタグ セレクタ
これらのセレクタは、VMM ドメインで「マイクロセグメンテーションを許可」する必要があるため、使用できません。

IP サブネット セレクタや IP アドレスを持つタグ セレクタなどの IP ベースのセレクタ
これらのセレクタは、EPG 内の分離、EPG 内のコントラクト、または VMM ドメインでの「マイクロセグメンテーションの許可」を使用して構成された、EPG 上のプロキシ ARP を必要とするため、使用できません。

例 13 : VMM ドメインのない EPG セレクタと IP ベースのセレクタ
次の例に示すように、セレクタの基準として IP アドレスを使用する場合は、プロキシ ARP が必要です。

- 例 5 : IP アドレスを介した VM エンドポイントの VMM 統合のないタグ セレクタ
- 例 7 : IP アドレスを介したベア メタル エンドポイントのタグ セレクタ
- 例 9 : IP サブネット セレクタ

プロキシ ARP を有効にするために、例 5 には次のオプションがリストされています。

- EPG 内分離を有効にしてから、プロキシ ARP を有効にする
- EPG 内コントラクトを構成すると、プロキシ ARP が暗黙的に有効になります

注 :　上記の 2 つのオプションに加えて、VMM 統合の「マイクロセグメンテーションを許可する」は、VMM 統合用に展開された VLAN に対して暗黙的にプロキシ ARP も有効にします。このような場合、この例で後述する考慮事項は適用されません。

EPG が ESG に一致する場合、これら 2 つを含むすべてのセキュリティ設定は、個々の EPG ではなく ESG を使用して実行する必要があるため、EPG セレクターが使用される場合、これらの 2 つのオプションに関する考慮事項があります。これは、ネットワークとセキュリティを切り離して、構成と設計を理解しやすく、維持しやすくするという ESG の哲学から生じています。問題は、ESG で内部 ESG 分離が有効になっている場合、ユーザーが一致した EPG でプロキシ ARP を有効にできるようになった場合でも、ESG 内のすべてのトラフィックがブロックされることです。一方、ESG 内の ESG 契約は、同じ ESG 内のトラフィックに契約ルールを適用しますが、EPG 内契約とは異なり、プロキシ ARP は内部で有効になりません。

これらの問題を解決するには、EPG セレクタと IP ベースのセレクタの両方を同時に使用する場合に、次の構成オプションを適用する必要があります。

1. EPG で EPG 内分離とプロキシ ARP を有効にします。
2. ESG で ESG 内の分離を有効にします。
    a. これにより、ステップ 1 の EPG 構成が、ステップ 4 の ESG によって上書きされなくなります。
3. ESG のデフォルト フィルタなど、すべてを許可する ESG 内契約を有効にします。
    a. これにより、手順 2 でブロックされている ESG 内のオープンな通信が可能になります。
4. EPG セレクタを使用して EPG を ESG に一致させます。

次の図は、この構成オプションのある例について説明します：

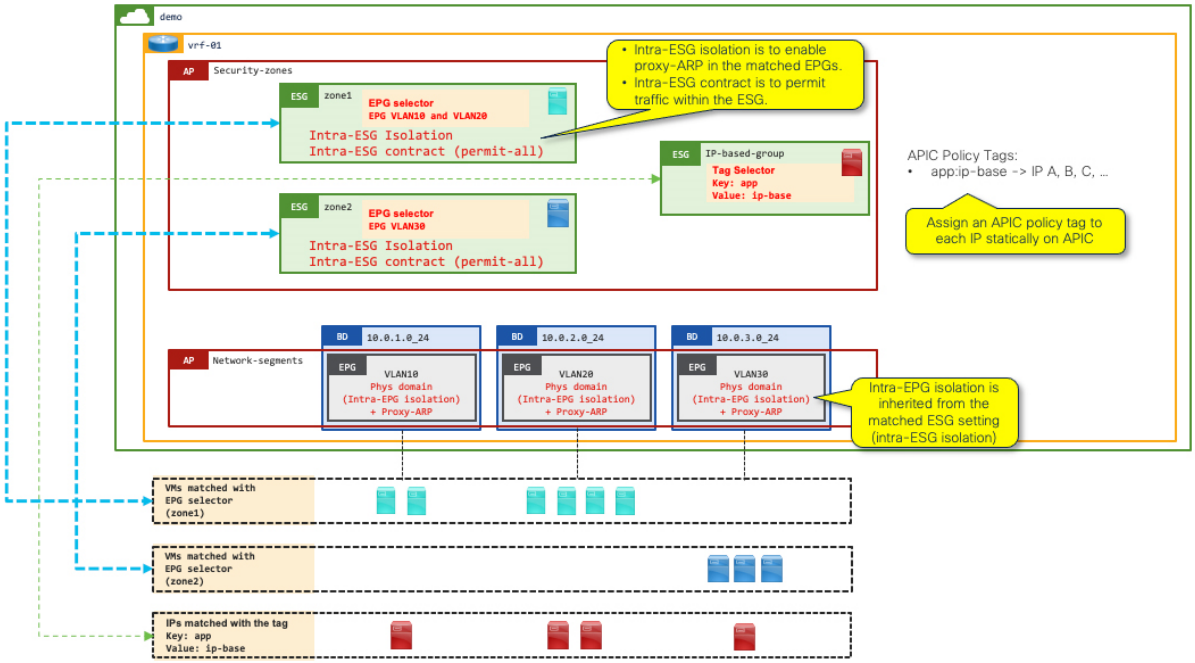


図 40. EPG セレクタと IP ベースのセレクタを同時に使用する場合の考慮事項

付録：ESG を使用した Cisco ACI テナントの設計例

この付録では、特定の VRF インスタンスのテナント間で Cisco ACI コンポーネント（VRF インスタンス / ブリッジ ドメイン / EPG / ESG）を配布するオプションについて説明します。これは主に、ESG がセキュリティに使用される場合に焦点を当てていますが、ほとんどの概念は ESG に関係なく適用できます。

次の表は、このセクションの Cisco ACI テナントの設計例をまとめたものです。次のサブセクションでは、各例について詳しく説明します。

表 4 Cisco ACI テナントの設計例

Category	例	テナント設計
テナント間のネットワークとセキュリティの分散	例 1：すべてがユーザー テナント内にある	VRF インスタンス、ブリッジ ドメイン、EPG、および ESG はユーザー テナントにあります
	例 2：VRF インスタンス / ブリッジ ドメイン / EPG（VLAN）はテナント*共通*であり、ESG はユーザー テナントにあります。	ネットワークとセキュリティの厳密な分離。 すべてのネットワーク - VRF インスタンス、ブリッジ ドメイン、および EPG（VLAN）はテナント*共通*です セキュリティ - ESG はユーザー テナントにあります
	例 3：VRF インスタンス / ブリッジ ドメインは*共通*テナントにあり、EPG（VLAN）と ESG はユーザー テナントにあります	ネットワークとセキュリティの分離が緩い。 基本ネットワーク - VRF インスタンス、ブリッジ ドメインはテナント*共通* EPG（VLAN）と ESG（セキュリティ）はユーザー テナントにあります
テナント間共有サービス	例 4：共有サービスは、テナント*共通*の同じ VRF インスタンスにあります	これは、テナント*共通*の同じ VRF インスタンスが複数のユーザー テナント間で共有される場合に適用されます。 VRF インスタンスとブリッジド メインは、共通テナントにあります EPG と ESG はユーザー テナント 2 にあります
	例 5：共有サービスが別の VRF インスタンスにある	テナント間のネットワークおよびセキュリティの分散に関係なく、共有サービスを独自の専用 VRF インスタンスに展開し、明示的な VRF インスタンス ルート リークを設定して接続を提供します。 VRF インスタンス、ブリッジ ドメイン、EPG および ESG は、ユーザー テナント 1 にあります。 VRF インスタンスと L3Out はユーザー tenant2 にあります

次の表は、テナントの設計オプションごとにサポートされている ESG セレクタをまとめたものです。

表 5　　Cisco ACI テナントの設計オプションとサポートされている ESG セレクタ

VRF	ブリッジ ドメイン	EPG	ESG	サポートされているセレクタ
テナント *共通*	テナント *共通*	テナント *共通*	テナント *共通*	タグセレクタ（Ep MAC） タグセレクタ（Ep IP） タグ セレクター（BD サブネット） タグ セレクター（静的エンドポイント） タグセレクタ（VM 名） タグセレクタ（VM タグ） IP サブネット セレクタ EPG セレクター
テナント *共通*	テナント *共通*	テナント *共通*	ユーザー テナント	タグセレクタ（Ep MAC）[1] タグセレクタ（Ep IP）[1] IP サブネット セレクタ
テナント *共通*	テナント *共通*	ユーザー テナント	ユーザー テナント	タグセレクタ（Ep MAC） タグセレクタ（Ep IP） タグ セレクター（静的エンドポイント） タグセレクタ（VM 名） タグセレクタ（VM タグ） IP サブネット セレクタ EPG セレクター
テナント *共通*	ユーザー テナント	ユーザー テナント	ユーザー テナント	タグセレクタ（Ep MAC） タグセレクタ（Ep IP）

				タグ セレクター（BD サブネット） タグ セレクター（静的エンドポイント） タグセレクタ（VM 名） タグセレクタ（VM タグ） IP サブネット セレクタ EPG セレクター
ユーザー テナント	ユーザー テナント	ユーザー テナント	ユーザー テナント	タグセレクタ（Ep MAC） タグセレクタ（Ep IP） タグ セレクター（BD サブネット） タグ セレクター（静的エンドポイント） タグセレクタ（VM 名） タグセレクタ（VM タグ） IP サブネット セレクタ EPG セレクター

脚注 1: ユーザー テナントのポリシー タグは、テナント***共通***のブリッジ ドメインまたは VRF インスタンスの名前を指定することにより、テナント***共通***の MAC または IP アドレスに割り当てることができます。ただし、ユーザー テナントに同じ名前のブリッジ ドメインまたは VRF インスタンスがある場合、ポリシー タグはブリッジ ドメインの MAC または IP アドレス、またはユーザー テナントの VRF インスタンスに割り当てられます。

例 ：ユーザー テナント内のすべて

この例は、すべてのオブジェクト、つまり VRF インスタンス、ブリッジ ドメイン、EPG、および ESG がユーザー テナントにある、最も一般的な使用例の 1 つです。ESG 間の契約も同じユーザー テナントにあります。

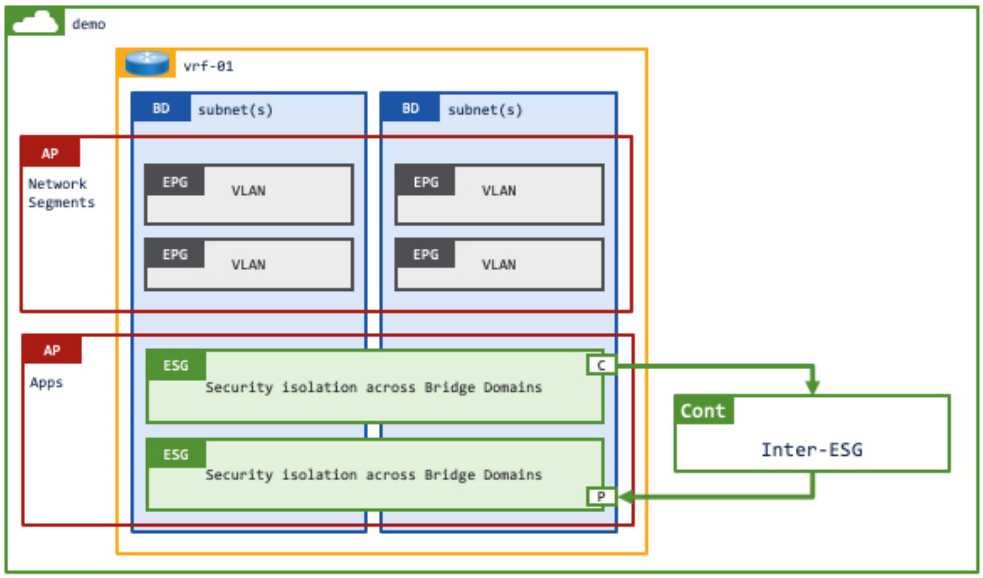


図 41. テナント内設計の論理図（VRF インスタンス、ブリッジ ドメイン、EPG および ESG はユーザー テナント内にあります）

例 2：VRF インスタンス / ブリッジ ドメイン / EPG（VLAN）はテナント共通、ESG はユーザー テナント

この例では、ユーザー テナントに ESG がありますが、VRF インスタンス、ブリッジ ドメイン、および EPG は共通のテナントにあります。ESG 間の契約は、同じユーザー テナントで定義されます。

EPG は EPG セレクタの ESG と同じテナントに属している必要があるため、この例では EPG セレクタを使用できません。

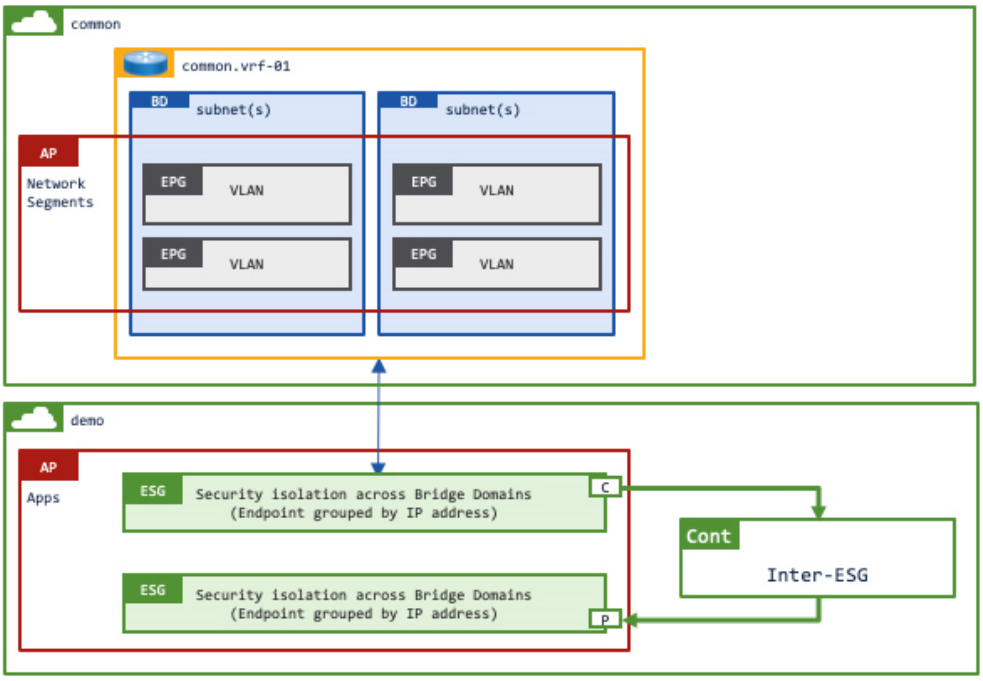


図 42. テナント内設計の論理図（VRF インスタンス、ブリッジ ドメイン、EPG は共通テナント内にあります）

例 3：VRF インスタンス / ブリッジ ドメインは共通テナントにあり、EPG（VLAN）と ESG はユーザー テナントにあります

この例では、ユーザー テナントに EPG と ESG があり、VRF インスタンスとブリッジ ドメインは共通テナントにあります。ESG 間の契約は、同じユーザー テナントで定義されます。

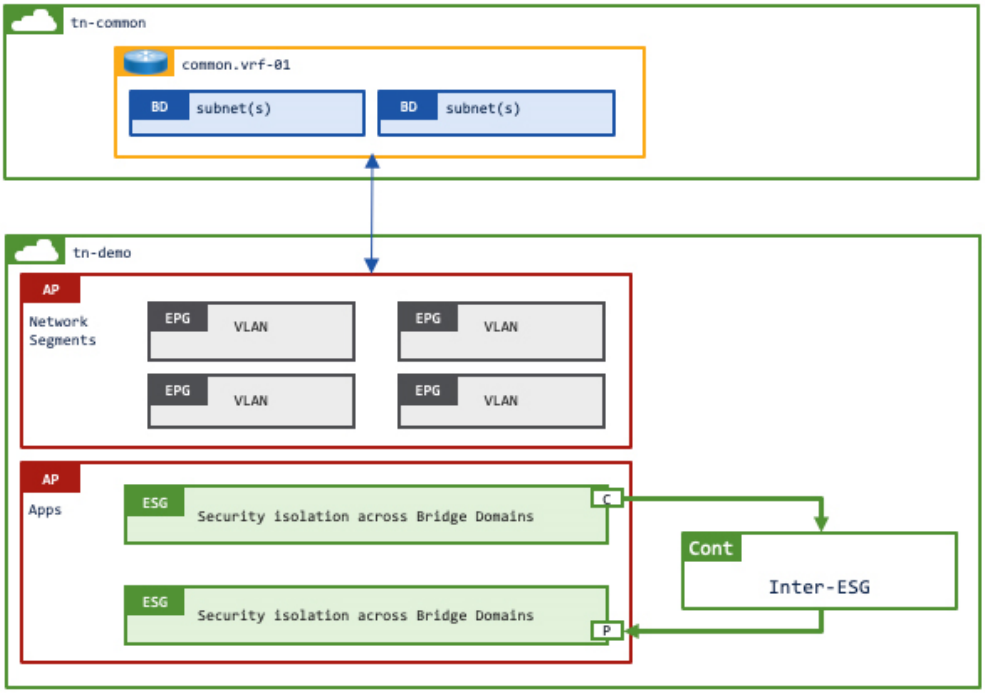


図 43. テナント内設計の論理図（VRF インスタンスとブリッジ ドメインは共通テナント内にあります）

例 4：テナント共通からの同じ VRF インスタンスの共有サービス

この例では、各ユーザー テナントに EPG と ESG がありますが、VRF インスタンスとブリッジ ドメインは共通のテナントにあります。この例ではテナント間契約を使用していますが、この例では引き続き、共通テナントの VRF インスタンスを使用して VRF インスタンス内通信を許可しています。したがって、ルート リークを構成する必要はありません。ESG 間のテナント間 VRF インスタンス コントラクトは、共通テナントまたはプロバイダー テナントで定義する必要があります。プロバイダー テナント内に契約が定義されている場合、契約を消費者テナント（図 45）にエクスポートする必要があります。

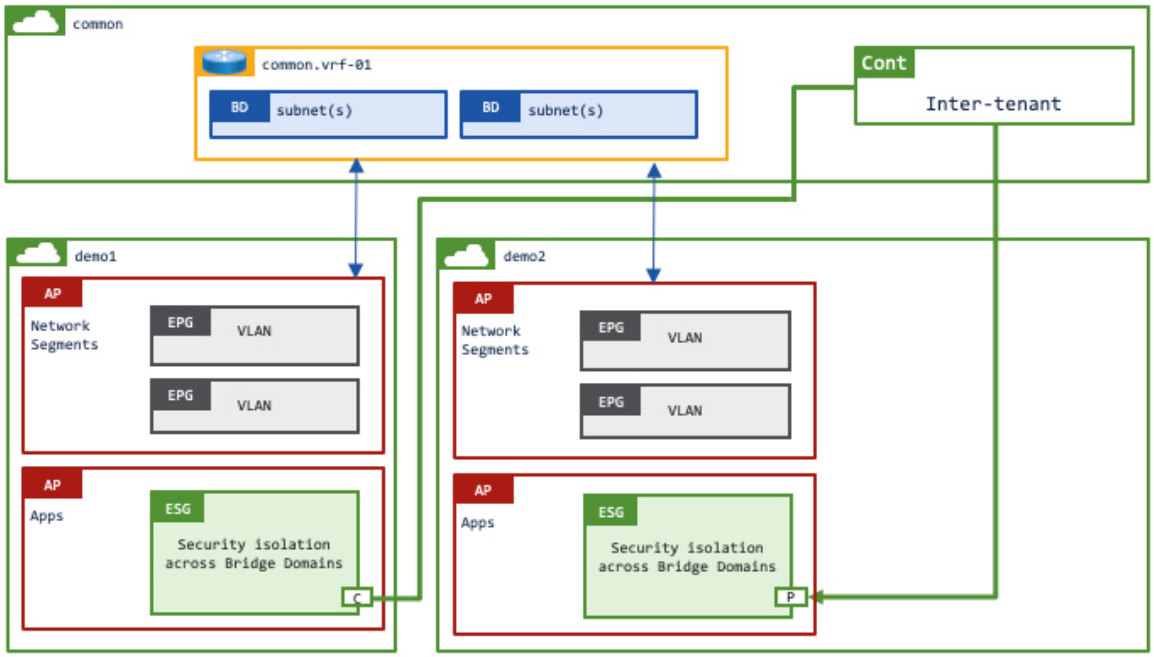


図 44. 共通テナント内ネットワーク構築によるテナント間 ESG 契約（契約は共通テナント内）

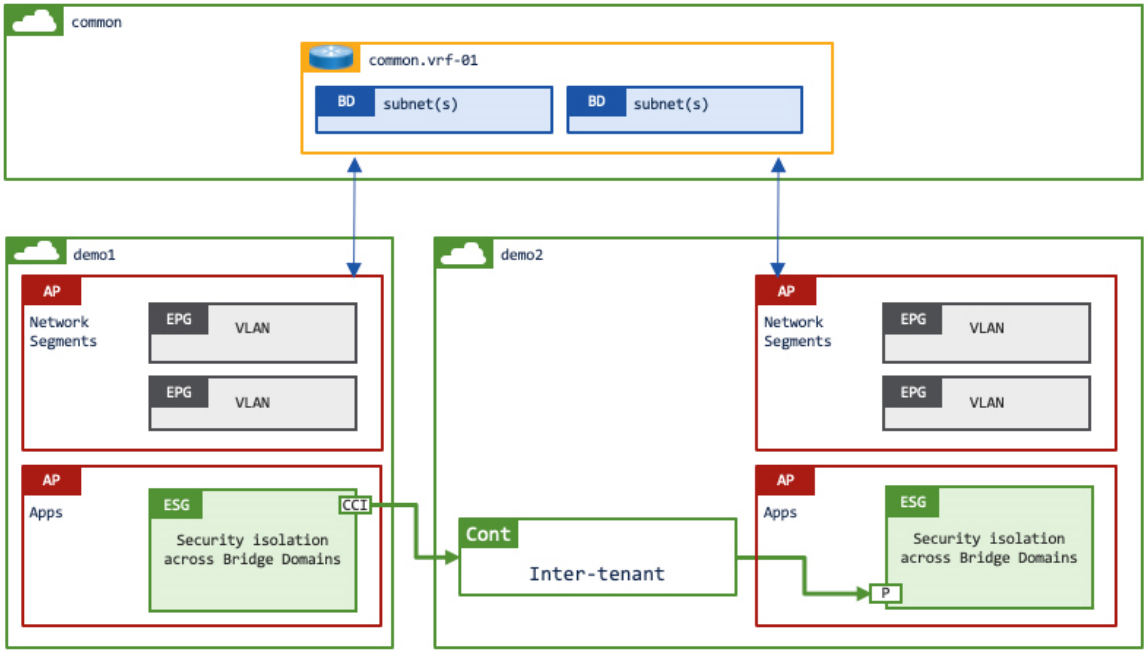


図 45. 共通テナント内ネットワーク構築によるテナント間 ESG 契約（契約はプロバイダーテナント内）

例 5 異なる VRF インスタンスの共有サービス

この例には、テナント***共通***の L3Out、または VRF インスタンス、ブリッジ ドメイン、EPG、および ESG を持つ別のユーザー テナントとのテナント間 VRF インスタンス契約を持つユーザー テナントがあります。L3Out 外部 EPG と ESG 間のテナント間 VRF インスタンス コントラクトは、共通テナントまたはプロバイダー テナントで

定義する必要があります。プロバイダー テナント内に契約が定義されている場合、契約を消費者テナント（図47）にエクスポートする必要があります。

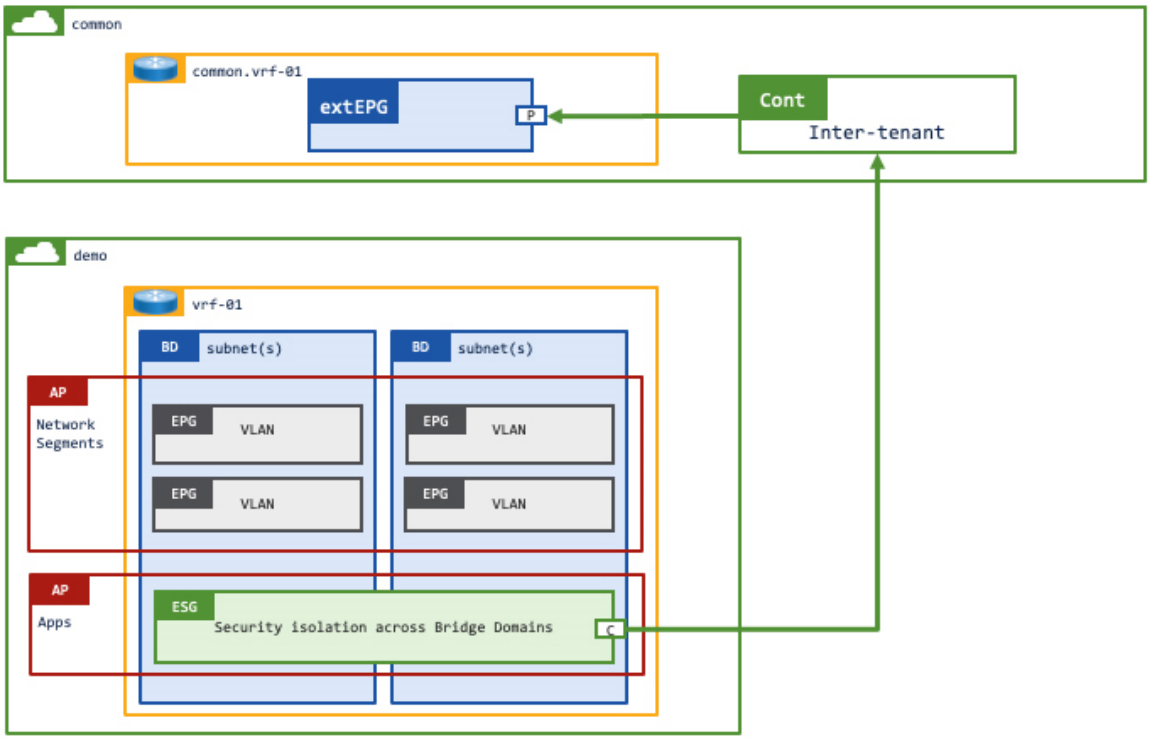


図 46. 共通テナントで L3Out を共有するテナント間 ESG 契約（契約は共通テナント内）

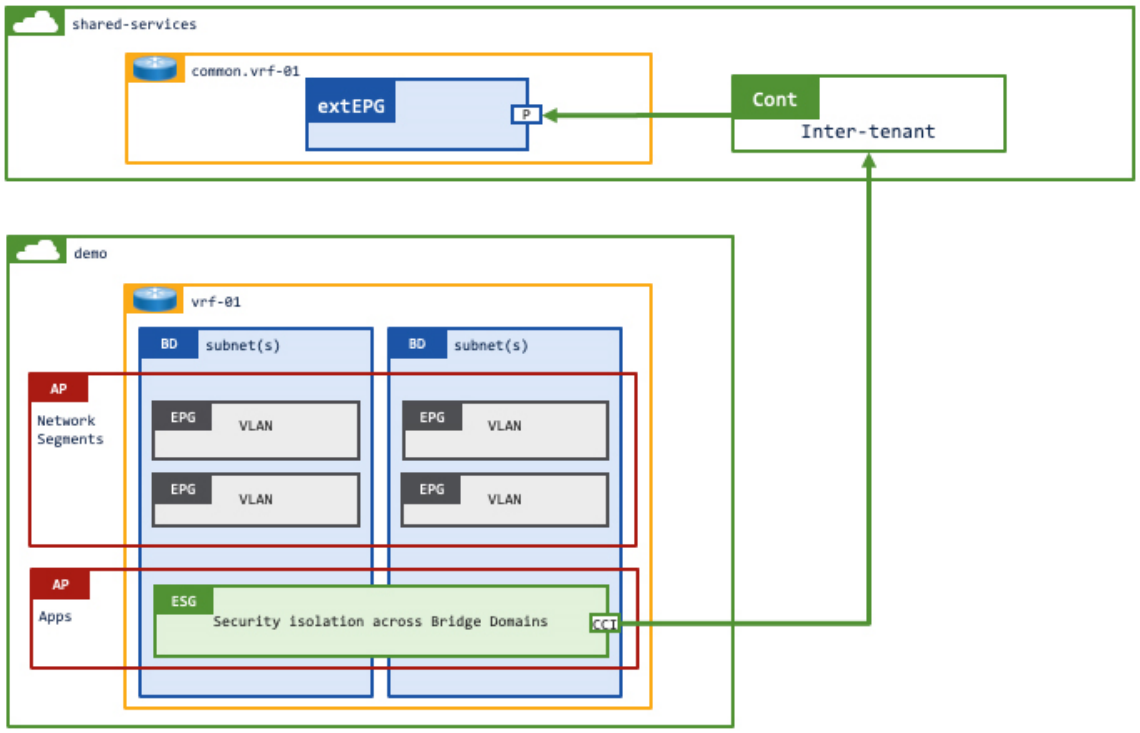


図 47. 別のユーザー テナントで L3Out を共有するテナント間 ESG 契約（契約はプロバイダー テナントにあります）

この例では、VRF 間インスタンスのルート リークが必要です。

ロケーションは、テナント > ネットワーク > VRF > VRF_name > ESG の VRF 間 リークされたルートにあります。

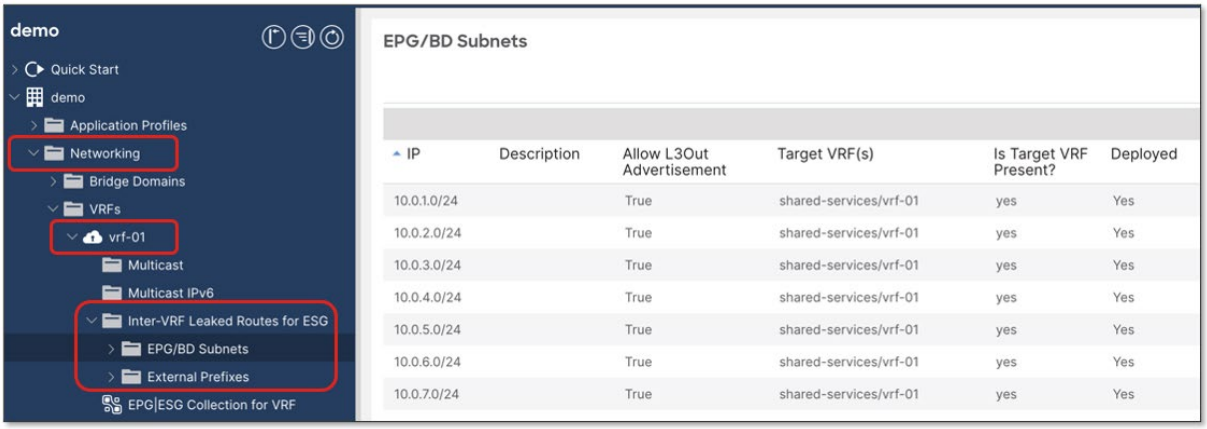


図 48. Inter-VRF インスタンス ルート リーク構成（tn-demo/vrf-01 から tn-shared-services/vrf-01 へ）

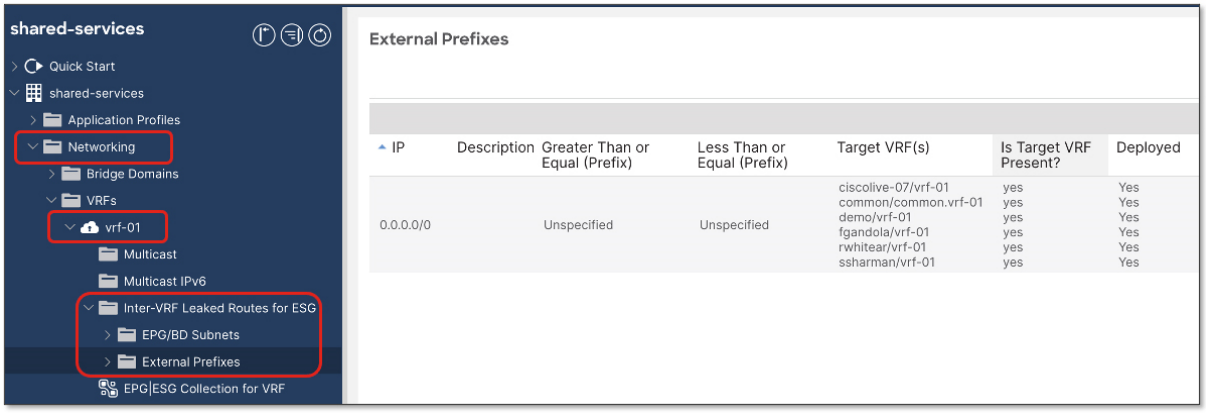


図 49. Inter-VRF インスタンス ルート リーク構成（tn-shared-services/vrf-01 から tn-demo/vrf-01 へ）

FAQ

このセクションは、よく寄せられる質問について説明します。

Q. サーバーと Cisco ACI リーフ ノードの間に中間スイッチがある場合はどうなりますか。

A. 「例 8：中間スイッチを備えたタグ セレクタ」セクションを参照してください。

Q. ESG と EPG 間の契約を構成できますか。

A. いいえ。 ESG を使用する場合、すべてのセキュリティは ESG で処理する必要があり、EPG は VLAN などのネットワーク構成にのみ使用する必要があります。EPG を ESG に移行する場合、EPG セレクタを使用できます。EPG セレクタを使用すると、ESG に移行した一致した EPG と、まだ ESG に移行していない他の EPG との間の通信が移行フェーズ中に許可されるように、一致した EPG から ESG に契約を継承できます。
ESG と契約の詳細については、以下のドキュメントを参照してください：

- 『Cisco APIC セキュリティ構成ガイド』の「エンドポイント セキュリティ グループ > 契約」
- 『Cisco APIC セキュリティ構成ガイド』の「エンドポイント セキュリティ グループ > ESG 移行戦略」

Q. ESG セレクタの Cisco APIC バージョンの最小要件は何ですか。

A. このドキュメントで説明されている ESG セレクタは、次のリリースからサポートされています。

EPG セレクタ – Cisco APIC リリース 5.2（1）

タグ セレクタ - Cisco APIC リリース 5.2（1）

IP サブネット セレクタ - Cisco APIC リリース 5.0（1）

『Cisco APIC セキュリティ構成ガイド』の「エンドポイント セキュリティ グループ > セレクタ」も参照してください。

Q. ESG の拡張性は、どうですか。

A. Cisco APIC の検証済み拡張性 ガイド のエンドポイント セキュリティ グループ（ESG）セクションを参照してください。

Q. EPG と比較して、ESG は TCAM 情報技術の使用率にどのように役立ちますか。

A. EPG または ESG との契約によって消費されるスイッチ上の TCAM 情報技術の量は、EPG / ESG と契約の数が同じ場合、同じです。ただし、ESG は、複数の EPG を 1 つの ESG に集約し、複数の EPG ではなく単一の

ESG から契約を消費 / 提供するなど、セキュリティ グループを作成するためのより柔軟なオプションを提供します。その結果、ESG を使用すると、スイッチでの TCAM 技術情報の使用を最適化できる場合があります。

Q. ESG セレクタの優先順位は何ですか。

A. 以下の表に優先順位を示します。これは、『Cisco APIC セキュリティ構成ガイド』の「エンドポイント セキュリティ グループ> セレクタの優先順位」にも記載されています。

表 6 スイッチされたトラフィックの優先順位

Precedence	セレクタ
1	タグ セレクター（エンドポイント MAC タグ） タグ セレクター（静的エンドポイント）
2	タグ セレクタ（VMM エンドポイント MAC タグ）
3	EPG セレクター

表 7 ルートされたトラフィックの優先順位

Precedence	セレクタ
1	タグ セレクター（エンドポイント IP タグ） IP サブネット セレクタ（ホスト IP）
2	タグ セレクタ（BD サブネット） IP サブネット セレクター（サブネット）
3	タグ セレクター（エンドポイント MAC タグ） タグ セレクター（静的エンドポイント）
4	タグ セレクタ（VMM エンドポイント MAC タグ）
5	EPG セレクター

Q. 読み取り専用と読み取り / 書き込み VMM ドメインの違いは何ですか。

A. VMware vCenter VMM ドメインには、次の統合オプションがあります。

- 読み取り / 書き込み VMM ドメイン（デフォルト オプション）では、ネットワーク管理者は単に EPG を VMM ドメインにマッピングします。ネットワーク コントローラ（Cisco APIC）は、VLAN プールから未使用の VLAN を選択し、ポートに面しているすべてのホストに VLAN を追加し、そしてアンシブル / テラフォームと同じ方法で VMware vCenter パブリックの API を通して EPG メイト正しい VLAN 識別子と一緒の VMware vDS にポート グループを構成します。このアプローチにより、物理ネットワークと vDS 間の VLAN の不一致のリスクが軽減されます。
  VM タグまたは VMware vCenter からの VM 名を持つ ESG タグ セレクタは、このモードでのみ使用できます。
- 読み取り専用の VMM ドメインでは、Cisco APIC のネットワーク管理者に VMware vCenter のポート グループ、VLAN、および VM の可視性を提供しながら、Cisco APIC の設定は VMware vCenter に伝達されず、明確な設定ドメインの分離が維持されます。このモードでは、ネットワーク管理者は、ポートに面するすべてのホストで特定の VLAN ID を使用して EPG を構成し、ネットワーク管理者は、管理者が同じ

VLAN 識別子を持つ vDS 上にポート グループを作成できるように、VMware vCenter 管理者に VLAN 識別子を通知します。

Q. トラフィック パスに挿入されるファイアウォールや IPS などのセキュリティ デバイスは、サブネットがセキュリティ グループの境界として使用されない可能性のあるアプリケーション中心の設計でセキュリティ グループをどのように識別しますか?

A. 現在、以下のアプリケーションとプラグインが ESG メンバーシップのアドバタイズに利用できます。

- Cisco 適応型セキュリティ アプライアンス（ASA）および Cisco Firepower Threat Defense（FTD）：Cisco ACI エンドポイントの更新
- Palo Alto Networks Panorama：Cisco ACI 用パノラマ プラグイン（ロードマップ）

レイヤ 4 からレイヤ 7 のサービス デバイスが上記のものと異なる場合、エンドポイントから ESG メンバーシップ情報は、Cisco APIC API を使用して取得できます。したがって、簡単なスクリプトまたはアプリケーションを使用して情報を取得し、レイヤ 4 からレイヤ 7 のサービス デバイスに同等のセキュリティ グループを作成できます。

次の API クエリは、特定の ESG からすべてのエンドポイントと関連する IP アドレスを取得します。

```
https://{{apic}}/api/mo/uni/tn-{{tenantName}}/ap-{{appProfileName}}/esg-
{{esgName}}.json?query-target=subtree&target-subtree-class=fvCEp&rsp-
subtree=children&rsp-subtree-class=fvIp
```

Cisco APIC の応答には、ESG に接続された各エンドポイントと、（利用可能な場合）エンドポイントの IP アドレスが含まれます：


```
{
    "fvCEp": {
        "attributes": {
            "annotation": "",
            "baseEpgDn": "uni/tn-demo/ap-network-segments/epg-192.168.52.x_24",
            "bdDn": "uni/tn-demo/BD-192.168.52.x_24",
            "childAction": "deleteNonPresent",
            "contName": "email-service",
            "dn": "uni/tn-demo/ap-online-boutique-hx/esg-all-services/cep-
00:50:56:A1:81:D3",
            "encap": "vlan-1206",
            "esgUsegDn": "",
            "extMngdBy": "",
            "fabricPathDn": "topology/pod-1/paths-102/pathep-[hx-dev-01-fi-b]",
            "hostingServer": "10.237.98.148",
            "id": "0",
            "idepdn": "",
            "lcC": "learned,vmm",
            "lcOwn": "local",
            "mac": "00:50:56:A1:81:D3",
            "mcastAddr": "not-applicable",
            "modTs": "2023-04-12T11:55:42.679+01:00",
```

```
                "monPolDn": "",
                "name": "00:50:56:A1:81:D3",
                "nameAlias": "",
                "reportingControllerName": "hx-dev-01-vc01.uktme.cisco.com",
                "status": "",
                "uid": "0",
                "userdom": "all",
                "uuid": "",
                "vmmSrc": "dvs",
                "vrfDn": "uni/tn-demo/ctx-vrf-01"
            },
            "children": [
                {
                    "fvIp": {
                        "attributes": {
                            "addr": "192.168.52.31",
                "annotation": "",
                            "baseEpgDn": "uni/tn-demo/ap-network-segments/epg-
192.168.52.x_24",
                            "bdDn": "uni/tn-demo/BD-192.168.52.x_24",
                            "bdDn": "uni/tn-demo/BD-192.168.52.x_24",
                            "createTs": "2023-04-12T12:00:43.000+01:00",
                            "debugMACMessage": "",
                            "esgUsegDn": "",
                            "extMngdBy": "",
                            "fabricPathDn": "topology/pod-1/paths-102/pathep-[hx-dev-01-
fi-b]",
                            "flags": "",
                            "lcOwn": "local",
                            "modTs": "2023-04-12T12:00:42.684+01:00",
                "monPolDn": "",
                            "rn": "ip-[192.168.52.31]",
                            "status": "",
                            "uid": "0",
                            "userdom": "all",
                            "userdom": "all",
                            "userdom": "all",
                        }
                }
            ]
        }
}
```


関連項目

- Cisco APIC リリース 6.0(x) セキュリティ設定ガイド
- エンドポイント セキュリティ グループ（ESG）により、ACI セグメンテーションと移行がより簡単に

- Cisco ACI ホワイト ペーパー

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。