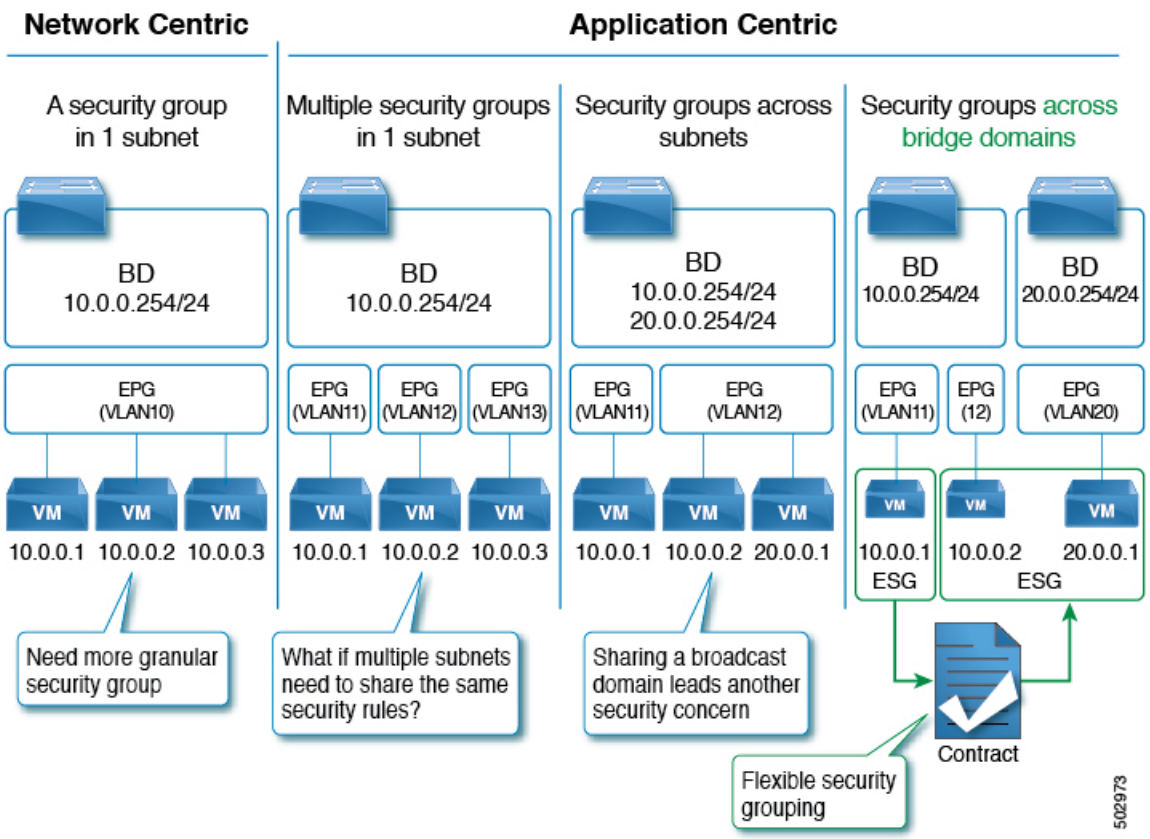
エンドポイント セキュリティ グループ

この章の内容は、次のとおりです。

エンドポイント セキュリティ グループについて

エンドポイントセキュリティ グループ（ESG）は、Cisco Application Centric Infrastructure（ACI）のネットワーク セキュリティ コンポーネントです。エンドポイントグループ（EPG）では Cisco ACI のネットワーク セキュリティを提供してきましたが、EPG は単一のブリッジドメインに関連付けられ、ブリッジドメイン内のセキュリティ ゾーンを定義するために使用する必要があります。これは、EPG が転送とセキュリティ セグメンテーションの両方を同時に定義するためです。ブリッジドメインと EPG の間の直接的な関係により、EPG が複数のブリッジドメインにまたがる可能性は制限されています。EPG のこの制限は、新しい ESG 構造を使用することで解決できます。

図 *1 : Cisco ACI* では、複数のセグメンテーション オプションを提供します



EPG を表すアプリケーション エンドポイントグループ（fvAEPg）オブジェクトは、レイヤ 2 ブロードキャストドメインを表すブリッジドメイン オブジェクト (fvBD) と直接関係があります。これは、上の図の最初の 3 列に示されています。

ESG は、物理または仮想ネットワークエンドポイントの収集を含む論理エンティティです。さらに、ESG はブリッジドメインではなく単一の VRF（仮想ルーティングおよび転送）インスタンスに関連付けられます。これにより、ブリッジドメインから独立したセキュリティ ゾーンの定義が可能になります（図 *1* の 4 番目の列は、この点を示しています）。EPG がブリッジドメインをセキュリティ ゾーンに分割するのと同様に、ESG は VRF インスタンスをセキュリティ ゾーンに分割します。

EPG ポリシーには、転送ロジックとセキュリティロジックの両方が組み込まれています。たとえば、EPG は、VLAN に基づくセキュリティゾーンだけでなく、リーフノードインターフェイスでの VLAN バインドも提供します。また EPG のコントラクトによってセキュリティを強化し、ブリッジドメイン サブネットを展開する必要があるリーフ ノードと、VRF ルート リーク（共有サービス）の場合にどのサブネットをどの VRF インスタンスにリークするかを決定するために使用されます。逆に、ESG はコントラクトによってセキュリティを強化するためにのみ使用され、転送ロジックは他のコンポーネントによって処理されます。ESG では、ブリッジドメイン サブネットの展開や VRF ルート リークなどのルーティング ロジックが VRF レベルに移動します。リーフノード インターフェイスの VLAN バインドは、引き続き EPG レベルで処理されます。

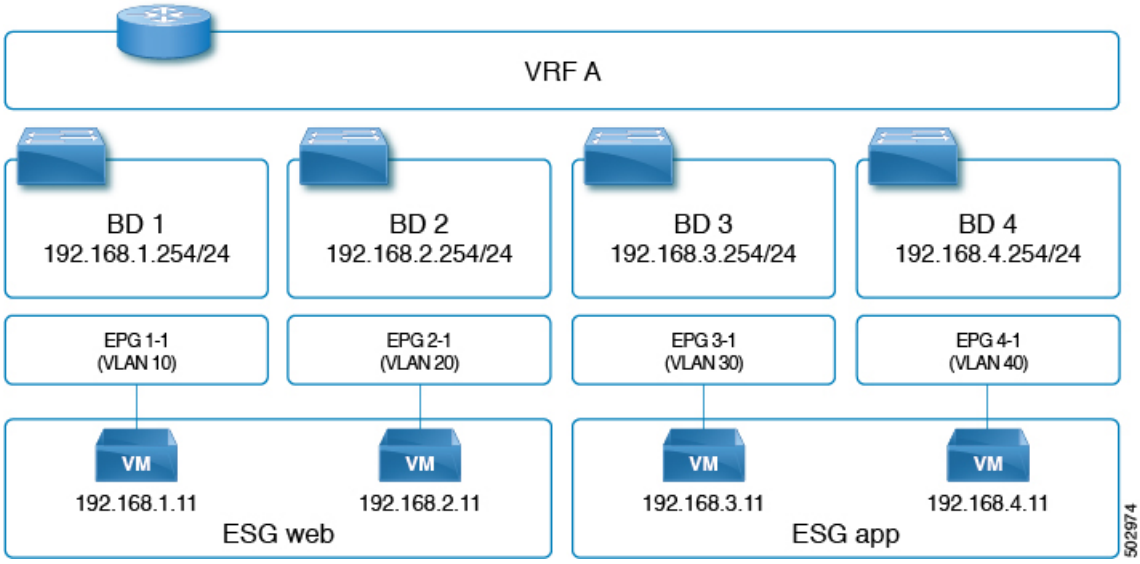
ESG はどのエンドポイントが ESG に属するかを定義する特定の一致基準を持つセキュリティ コンストラクトであり、コントラクトまたはポリシーを使用してセキュリティスタンスを定義します。一致基準は、関連付けられた VRF インスタンスのブリッジドメインにまたがる IPv4 または IPv6 アドレス、またはエンドポイント MAC アドレスに関連付けられたタグなどの属性に基づく ESG セレクタと呼ばれます。これらのセレクタおよびその他のサポートされているセレクタタイプの詳細については、「セレクターについて （6 ページ）」 を参照してください。

ESG でのコントラクトの使用は、EPG と同じです。同じ ESG に属するエンドポイントは、コントラクトを必要とせずに通信できます。異なる ESG に属するエンドポイント間の通信を有効にするには、ESG 間のコントラクトを構成する必要があります。Cisco ACI ファブリックの外部にあるデバイスと通信するには、L3Out 外部 EPG（`l3extInstP`）と ESG の間のコントラクトを構成する必要があります。ESG 間のコントラクトと組み合わせて、レイヤ 4 ～ レイヤ 7 サービスグラフを使用することもできます。ただし、EPG と ESG 間のコントラクトはサポートされていません。

ESG から ESG へのトラフィック フィルタリング

次の図では、4 つのブリッジ ドメインがそれぞれ 1 つの EPG に関連付けられています。管理者は EPG 設定を使用して、仮想マシンまたは物理サーバーからのトラフィックが、適切な VLAN に接続された適切なブリッジ ドメインに関連付けられていることを確認します。たとえば、EPG1-1 は VLAN 10 からのトラフィックの BD1 へのマッピングを定義し、EPG2-1 は VLAN 20 を BD2 にマッピングします。

図 *2: ESG* を使用して、異なるサブネットのエンドポイントを集約できます



- VLAN 10 の 192.168.1.11 と VLAN 20 の 192.168.2.11 は、異なるサブネットと異なるブリッジ ドメインに属しています。
- 管理者は、192.168.1.11 と 192.168.2.11 を同じ ESG に属するものとして定義します。

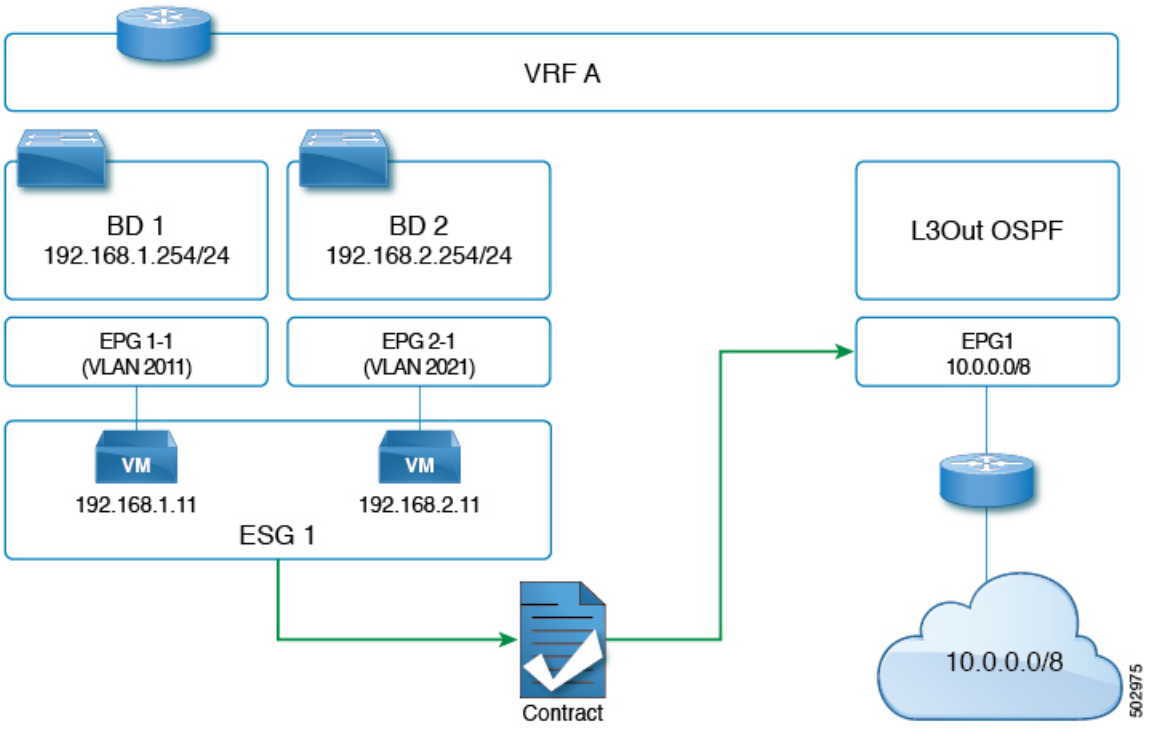
- 同様に、192.168.3.11 と 192.168.4.11 はそれぞれ BD3 と BD4（EPG3-1 と EPG4-1 経由）に関連付けられており、両方とも同じ ESG に属しています。
- 上記の設定により、192.168.1.11 は 192.168.2.11 と自由に通信できます。
- 同様に、192.168.3.11 は 192.168.4.11 と通信できます。ただし、192.168.1.11（または 192.168.2.11）は、契約なしでは 192.168.3.11 または 192.168.4.11 のいずれとも通信できません。

（注） EPG によって使用される契約は、ESG によって再利用できません。その逆も同様です。

外部から ESG へのトラフィック フィルタリング

外部から ESG への通信を許可する設定は、次の図に示すように、L3Out 外部 EPG（`l3extInstP`）と ESG 間の契約によって実行されます。L3Out の観点からは、ESG との契約と EPG との契約の間に違いはありません。

図 *3 : ESG* から外部への接続は、*L3* 外部 *EPG* を使用して実装されます。



ESG の導入

このセクションでは、管理者が ESG を設定する場合に、Cisco APIC によってリーフノードをプログラムする方法をまとめます。

- 各 ESG は VRF に関連付けられており、ESG セレクタは VRF 内のどのエンドポイントが ESG に属するかを定義します。
- VRF（ESGが設定されている場所）は、入力または出力ポリシー適用モードで構成できます。
- Cisco ACI は、関連付けられた VRF が展開されているすべてのリーフノードで ESG 構成をインスタンス化します。
- ESG が構成されている場合、関連付けられた VRF 内のすべての BD サブネットは、その VRFが存在するすべてのリーフノード上で、スパインプロキシへの静的ルートとして存在します。
- ESGは常にオンデマンドの即時展開によって展開され、関連するコントラクトルールは、ESGセレクタに一致するエンドポイントが特定のリーフノードで学習された後にのみプログラムされます。
- ESG 間のコントラクトは、EPG の場合と同様に、リーフノード TCAM の policy-cam ルールとしてプログラムされます。
- ESGによって使用されるクラスIDは、グローバルpcTagです。コンテキストによっては、sclass と呼ばれます。
- EPG とは異なり、ESG 間のコントラクトはセキュリティルールのみを作成します。ESG は、サブネット展開やルートリークなどのネットワーク展開には使用されません。
- EPG、BD、およびVRFコンストラクトは、ネットワーク フォワーディング コンストラクトに対して通常どおり構成する必要があります。ただし、セキュリティ定義は、EPGからアプリケーション中心のセキュリティを適用する ESG に移動されます。このようなシナリオでは、EPG の機能は VLAN をインターフェイスにバインドすることです。

（注） Cisco APIC は、EPG の場合と同様に、各 ESG を識別するため固有の番号を生成します。この番号は、pcTag またはクラス ID と呼ばれます。一部のコンテキストでは、sclass、S クラス、またはソースクラスと呼ばれます。

グローバル pcTag は、ESG（または EPG）が属する VRF に関係なく、ファブリック全体で固有の番号です。ESG には常にグローバル pcTag が割り当てられます。グローバル pcTag 番号の範囲は 16 ～ 16385 です。

ローカル pcTag は、VRF 範囲内で固有の番号です。つまり、Cisco APIC は同じ番号を生成して、異なる VRF 内の別の EPG を識別できます。ローカル pcTag 番号の範囲は 16386 ～ 65535 です。

1 から 15 までの pcTag 番号は、システム内部で使用するために予約されています。

セレクタ

セレクターについて

セレクタは、エンドポイントを ESG に分類するためのさまざまなマッチング基準を使用し、各 ESG の下に構成されます。VLAN を使用してエンドポイントを分類する EPG とは異なり、ESGはより柔軟な基準を使用してエンドポイントを分類できます。この概念は、マイクロセグメンテーション EPG（または useg EPG）に似ています。ただし、useg EPG は 1 つのブリッジドメインに関連付けられたままですが、ESGにはブリッジドメイン全体のエンドポイントを含めることができます。

サポートされている ESG セレクタは次のとおりです。

- **タグセレクタ**：MAC および IP アドレス、仮想マシン（VM）タグ、仮想マシン名（vm 名）、サブネットタグ、静的エンドポイントタグなどのさまざまな属性に割り当てられたポリシータグに基づいてエンドポイントをマッチングします。ESG タグセレクタは、ESG と同じテナントのポリシータグのみとマッチングできます。タグセレクタは Cisco APIC リリース 5.2(1) で導入されました。
- **EPG セレクタ**：特定の EPG 内のすべてのエンドポイントとマッチングし、ESG は EPG の下で構成されたすべてのコントラクトを継承します。このセレクタを使用すると、ユーザーはセキュリティ構成を EPG から ESG にシームレスに移行できます。ESG は、ESG と同じ VRF 内の EPG に対してのみ EPG セレクタを使用できます。EPG セレクタは、Cisco APIC リリース 5.2(1) で導入されました。
- **IP サブネットセレクタ**：ホストの IP アドレスまたは IP サブネットに基づいてエンドポイントをマッチングします。タグセレクタは、ポリシータグを介して同じ機能を提供します。IP サブネットセレクタは、Cisco APIC リリース 5.0(1) で導入されました。
- **サービス EPG セレクタ**：サービス EPG セレクタは、Cisco APIC リリース 5.2(4) で導入されました。

  サービス EPG は、デバイス選択ポリシーのコネクタに基づいて ACI が自動的に作成する EPG です。サービス グラフ リダイレクトに基づくほとんどの展開では、ACI がトラフィックをレイヤ 4 からレイヤ 7 デバイスにリダイレクトするため、レイヤ 4 からレイヤ 7 デバイスに直接送信されるトラフィックを許可または拒否するために特別なことを構成する必要はありません。レイヤ 4 からレイヤ 7 のデバイス IP アドレスにトラフィックを直接送信する必要がある場合は、サービス EPG へのトラフィックを許可または拒否する必要がある場合があります。サービス EPG セレクタを使用すると、サービス EPG をサービス ESG にマッピングできるため、管理者は、サービス グラフを介して展開されたレイヤ 4 からレイヤ 7 デバイスにトラフィックを送信できる ESG をより細かく制御できます。

タグ セレクターについて

タグセレクタはポリシータグを使用して、エンドポイントを特定の ESG に分類します。ポリシー タグは、「キー：所有者、値：ジョン」などのキーと値で構成されます。ポリシー タグ

は、ユーザが構成可能なさまざまなオブジェクトに割り当てることができ、Cisco Application Centric Infrastructure（ACI）機能はそれらのタグに基づいて動作します。ポリシータグを使用したセキュリティ分類は、複数のエンドポイントをセキュリティグループ(ESG)に追加するために簡単で直感的な操作ができます。ポリシータグと ESG タグセレクタを使用すると、各エンドポイントを個別に指定することなく、選択した複数のエンドポイントを ESG に分類できます。

ESG タグ セレクタは、ESG と同じテナントのポリシータグのみに一致します。この分離により、各テナントが独自のリソースを管理できるようになり、テナント間での意図しないポリシータグの一致が防止されます。ただし、ユーザ テナントがブリッジドメインまたは `Common` テナントからの VRF インスタンスを使用している場合、ユーザ テナントは構成を一部表示できない場合があることに注意してください。

構成は似ていますが、ポリシータグ（ユーザー定義可能な tagTag など）は、注釈（tagAnnotation）とは目的と使用方法が異なります。相違点の詳細については、*Cisco APIC System Management Configuration Guide*の「Alias, Annotations, and Tags」の章を参照してください。

ESG タグセレクタは、次のオブジェクトに割り当てられたポリシータグと一致します。

名前	説明	オブジェクト
BD サブネット	ブリッジドメインの下のサブネット	fvSubnet
IP エンドポイントタグ	エンドポイントのホスト IP アドレスのメタデータ	fvEpIpTag
MAC エンドポイントタグ	エンドポイントの MAC アドレスのメタデータ	fvEpMacTag
VMM MAC エンドポイントタグ	VMM 統合を介して派生したメタデータ	fvEpVmmMacTagDef
静的エンドポイント	静的エンドポイント	fvStCEp

（注） 仮想マシンを名前で選択する場合、仮想マシンが ESG に関連付けられる前に、VM が関連付けられている EPG の EPG セレクタを作成する必要があります。

次のセクションでは、サポートされているオブジェクトの各タイプのポリシータグの使用について説明します。

BD サブネットのポリシータグ

ブリッジドメインサブネットに割り当てられたポリシータグを照合することにより、タグセレクタはサブネット内のすべての IP エンドポイントを特定の ESG に分類できます。IP サブネットセレクタに似ていますが、ポリシータグとタグ セレクタを使用すると、特定の MAC アドレ

スなどのさまざまなタイプのパラメータに加えて、複数の IP サブネットをグループ化できます。

また、[**デフォルトの SVI ゲートウェイなし（No Default SVI Gateway**）] オプションを使用してより小さい BD サブネットを作成し、その小さいサブネットにポリシータグを割り当てることにより、BD サブネットのサブセットを一致させることができます。このオプションを使用すると、対応する SVI を展開せずにブリッジドメインの下にサブネットを構成できます。

BD サブネットのポリシータグに一致するタグセレクタを構成する場合は、次の注意事項を考慮してください。

- タグセレクタは、別のテナントの BD サブネットのポリシータグと一致させることはできません。たとえば、ESG がテナント「A」にあり、ブリッジドメインがテナント `Common` で構成されている場合、テナント「A」のタグ セレクタは、そのブリッジドメインのポリシータグと一致させることはできません。このようなケースでサブネットベースの分類が必要な場合は、代わりに IP サブネットセレクタを使用します。
- EPG サブネットの下のポリシータグは、ESG タグセレクタではサポートされていません。ESG では、EPG の下にサブネットを構成する必要はありません。ESG は、以前は EPG に結合されていたネットワークとセキュリティの構成を分離することにより、構成を簡素化することを目的としています。
- BD サブネットのポリシー タグに一致するタグ セレクタは、エンドポイントの IP アドレスのみを ESG に分類し、MAC アドレスは分類しません。このため、ここでは IP ベースのセレクタによるレイヤ 2 トラフィック制限が適用されます。詳細については、IP ベースセレクターによるレイヤー 2 トラフィック制限 （23 ページ）を参照してください。

IP エンドポイントタグのポリシータグ

エンドポイント（fvCEp、fvIp）を表すオブジェクトは、Cisco ACI スイッチのエンドポイント学習ステータスに基づいて動的に作成および削除されるため、そのようなオブジェクトにポリシー タグを直接割り当てることは実用的ではありません。そのため、エンドポイントの IP アドレスを表すために、新しいユーザによって構成可能なオブジェクトである IP エンドポイント タグが Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(1) で導入されました。IP エンドポイントタグ オブジェクトは、IP アドレスがエンドポイントとして学習される前でも作成し、維持できます。このオブジェクトを使用すると、いつでもエンドポイントの IP アドレスにポリシータグを割り当てることができます。

IP エンドポイントタグには VRF の範囲があり、特定の VRF で構成したホスト IP アドレスを表します。タグは、IP アドレスのメタデータまたは記述子です。IP エンドポイントタグを構成しても、エンドポイントまたは指定された IP アドレスは展開されません。エンドポイントが学習される前にエンドポイントとその IP アドレスを静的に展開する必要がある場合は、静的エンドポイントを構成します。

IP エンドポイントタグのポリシータグに一致するタグセレクタを構成するときは、次の注意事項を考慮してください。

- IP エンドポイントタグのポリシータグに一致するタグセレクタは、エンドポイントの IP アドレスのみを ESG に分類し、MAC アドレスは分類しません。このため、ここでは IP

ベースのセレクタによるレイヤ 2 トラフィック制限が適用されます。詳細については、IP ベース セレクターによるレイヤー 2 トラフィック制限 （23 ページ）を参照してください。

MAC エンドポイントタグのポリシータグ

エンドポイント（fvCEp、fvIp）を表すオブジェクトは、Cisco ACI スイッチのエンドポイント学習ステータスに基づいて動的に作成および削除されるため、そのようなオブジェクトにポリシー タグを直接割り当てることは実用的ではありません。そのため、エンドポイントの MAC アドレスを表すために、新しいユーザによって構成可能なオブジェクトである MAC エンドポイント タグが Cisco APIC リリース 5.2(1) で導入されました。MAC アドレスをエンドポイントとして学習する前でも、MAC エンドポイント タグオブジェクトを作成し、維持できます。このオブジェクトを使用して、いつでもエンドポイントの MAC アドレスにポリシータグを割り当てることができます。

MAC エンドポイント タグにはブリッジドメインの範囲があり、特定のブリッジドメインで構成した MAC アドレスを表します。MAC アドレスがブリッジドメイン全体で固有の場合は、ブリッジドメインの範囲を「任意」（「*」）として指定し、代わりにその範囲として VRF を提供できます。タグは、MACアドレスの単なるメタデータまたは記述子です。MACエンドポイントタグを構成しても、エンドポイントまたは指定された MAC アドレスは展開されません。エンドポイントが学習される前にエンドポイントとその MAC アドレスを静的に展開する必要がある場合は、静的エンドポイントを構成します。

VMM MAC エンドポイントタグのポリシータグ

Cisco APIC は VMM 統合を通じて学習した情報に基づいて、読み取り専用の VMM MAC エンドポイント ポリシー タグ（fvEpVmmMacTagDef）を自動的に入力します。Cisco APIC は VMM 統合を通じてエンドポイントに関する情報を取得し、その情報を各エンドポイントのポリシータグにマップします。手動で作成する MAC エンドポイント タグオブジェクトと同様に、VMM MAC エンドポイント タグオブジェクトは、対応するエンドポイントがデータプレーンでまだ学習されていない場合でも、ポリシータグを維持するための MAC アドレスの単なるメタデータまたは記述子です。ESG タグセレクタは、これらのポリシータグを使用して、エンドポイントを ESG に分類できます。

次の VMM 情報は、ESG タグセレクタによってサポートされます。

統合のタイプ	出典情報	翻訳されたポリシータグの形式
VMware vSphere 分散スイッチ（vDS）	VM 名	キー：`__vmm::vmname` 値：*VM name*
VMware vSphere 分散スイッチ（vDS）	vSphere タグ 「カテゴリ：タグ名」	キー：カテゴリ 値：タグ名

VMM MAC エンドポイントタグと VM の名前から変換されたポリシータグは、Cisco APIC の **[テナント（Tenant）] > [ポリシー（Polices）] > [エンドポイント タグ（Endpoint Tags）] > [エ**

ンドポイント MAC（Endpoint MAC）] の下に自動的に入力されます。これを有効にするには、VMM ドメインを EPG に関連付けるときに **[マイクロセグメンテーションを許可（Allow Micro-Segmentation）]** を有効にする必要があります。これらのタグは、手動で構成された MAC エンドポイントタグと区別するために、サフィックス「（VMM）」を付けて表示されます。VMware タグなど、VM の名前以外で翻訳されたポリシータグは、ESG タグセレクタで一致するまで VMM MAC エンドポイントタグで生成されません。また、対応する VMM ドメインで**タグコレクション**を有効にする必要があります。変換された各ポリシータグは、エンドポイントの MAC アドレスに割り当てられます。

MAC エンドポイント タグが、VMM MAC エンドポイント タグと同じブリッジドメインの同じ MAC アドレスで構成されている場合、MAC エンドポイント タグのポリシー タグのみが使用されます。この場合、VMM MAC エンドポイントタグからの変換されたポリシータグは無視されます。

静的エンドポイントのポリシータグ

EPG で構成された静的エンドポイントに割り当てられたポリシータグを照合することにより、タグセレクタは静的エンドポイントの MAC アドレスを特定の ESG に分類できます。静的エンドポイントのポリシータグサポートにより、静的エンドポイントと同じ MAC アドレスに MAC エンドポイントタグを構成する必要がなくなります。実際、これら 2 つの構成は互いに互換性がありません。まとめると、次のようになります。

- ポリシー タグが静的エンドポイントに割り当てられている場合、同じブリッジドメインで同じ MAC アドレスを持つ MAC エンドポイント タグを構成することはできません。
- MAC エンドポイント タグが MAC アドレスに割り当てられている場合、ポリシー タグを同じブリッジドメイン内の同じ MAC アドレスを持つ静的エンドポイントに割り当てることはできません。

静的エンドポイントタグは、**silent-host** タイプの静的エンドポイントに対してのみサポートされます。

EPG セレクターについて

EPG セレクタは、EPG 全体を ESG に一致させます。EPG セレクタを使用して複数の EPG を ESG に一致させることができますが、それは EPG が ESG と同じテナントおよび同じ VRF にある場合のみです。EPG セレクタは、ブリッジドメインにまたがる複数の VLAN を単一のセキュリティグループ（ESG）としてグループ化し、コントラクトの構成を簡素化するのに最適です。

EPG が EPG セレクタによって ESG に一致すると、EPG 内のすべてのエンドポイントが ESG に属し、すべてのセキュリティ構成が ESG によって処理されるようになりました。

EPG セレクタには次の特徴があります。

- EPG に基づく既存のコントラクトは、ESG によって継承されます。
- EPG は新しいコントラクトを消費または提供できません
- EPG 内分離は、ESG 内の ESG 内分離によって上書きされます。

• EPG の優先グループメンバーシップは、ESG によって上書きされます。

EPG が EPG セレクタを介して ESG に一致する場合、EPG と ESG の下での EPG 内/ESG の分離と優先グループメンバーシップの設定は同じである必要があります。一致後、ESG 設定は EPG 設定を上書きします。

EPG から ESG へのコントラクトの継承により、既存の EPG セキュリティ設計から新しい ESG セキュリティ設計へのシームレスな移行が可能になります。構成を簡素化して ESG の利点を十分に活用するために、移行を完了し、EPG から ESG への通信のために継承された EPG コントラクトを永続的な構成として保持しないことをお勧めします。ESG に EPG セレクタによって継承されたコントラクトがある場合、APIC は EPG から ESG への移行がまだ完了していないことを示す警告とリマインダとしてエラーを発生させます。EPGセレクタを使用した移行の詳細については、「ESG 移行計画」セクションを参照してください。

EPG が EPG セレクタによって ESG に一致すると、EPG のポリシー制御タグ（pcTag）が ESG の pcTag に置き換えられます。pcTag の置換操作により、EPG のエンドポイントで一時的なトラフィックの小規模の中断が発生する場合があります。これは、EPG で共有サービス（ルートリーク）を構成する場合など、他の機能で発生する他の pcTag 更新イベントと同じ影響があります。pcTag は ESG に固有ではなく、タグセレクタによって使用されるポリシータグ（tagTag）とは関係がないことに注意してください。pcTag は、データプレーンでコントラクトを適用するための EPG/ESG 識別子です。

IP サブネット セレクターの詳細

IP サブネット セレクターは、IP アドレスに基づいてエンドポイントを ESG に分類します。特定のエンドポイントに一致するようにホスト IP アドレスを設定するか、サブネット内の複数の IP アドレスに一致するようにサブネットを設定できます。

IP エンドポイント タグ セレクターは、エンドポイントの IP アドレスのみを ESG に分類し、MAC アドレスは分類しません。このため、ここでは IP ベースのセレクターによるレイヤー 2 トラフィック制限が適用されます。詳細については、「*IP* ベースのセレクターによるレイヤー *2* トラフィックの制限」を参照してください。

サービス EPG セレクターについて

リリース 5.2(4) より前のリリースでは、サービスグラフを通じて作成されたサービス EPG とのコントラクトを作成することはできません。この制限には、次のような特定の課題があります。

- [**直接接続（Direct Connect**）] オプションを使用して、サービス EPG からコンシューマーまたはプロバイダー EPG へのトラフィックの許可ルールを追加できます。ただし、コンシューマーやプロバイダー EPG ではない EPG は、vzAny コントラクトまたは優先グループをあわせて構成しなければ、サービス EPG と通信できません。
- vzAny にはサービス EPG が含まれているため、vzAny から vzAny へのコントラクトは、サービス EPG と VRF 内の他の EPG との間のトラフィックを許可できます。ただし、これは VRF 内の他のすべての EPG がサービス EPG と通信できることも意味しますが、VRF 内の特定の EPG のみを制限してサービス EPG と通信できるようにする必要がある場合もあります。

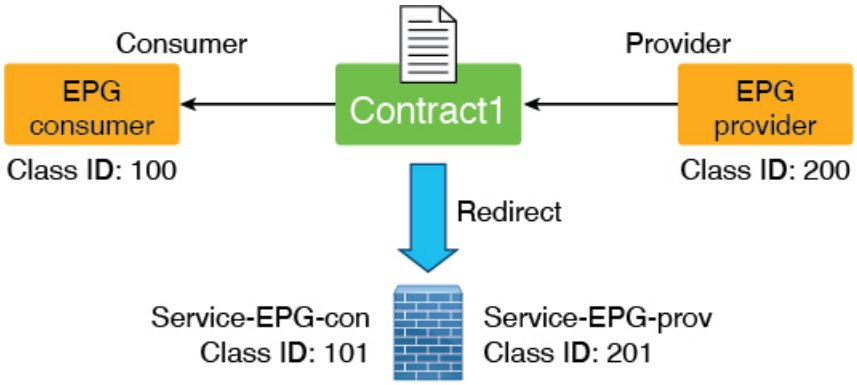
リリース 5.2(4) 以降のリリースでは、エンドポイントセキュリティ グループ (ESG) のサービス EPG セレクタが使用できるようになりました。この機能により、サービス EPG を ESG にマッピングし、その ESG とのコントラクトを作成できます。この機能を使用すると、vzAny-to-vzAny 許可コントラクトが構成されている場合でも、サービス ESG と他の ESG の間に拒否コントラクトを追加して、特定の ESG がサービス ESG と通信できるようにすることができます。

次のセクションでは、サービス EPG セレクタを使用する場合と使用しない場合の構成例と、サービス EPG セレクタの使用に関する追加情報について説明します。

- サービス EPG セレクタを使用しない構成例 （12 ページ）
- サービス EPG セレクタを使用した構成例 （16 ページ）
- ESG およびサービス EPG のサポートされている場所とサポートされていない場所 （18 ページ）
- サービス EPG セレクタの注意事項と制限事項 （22 ページ）

サービス EPG セレクタを使用しない構成例

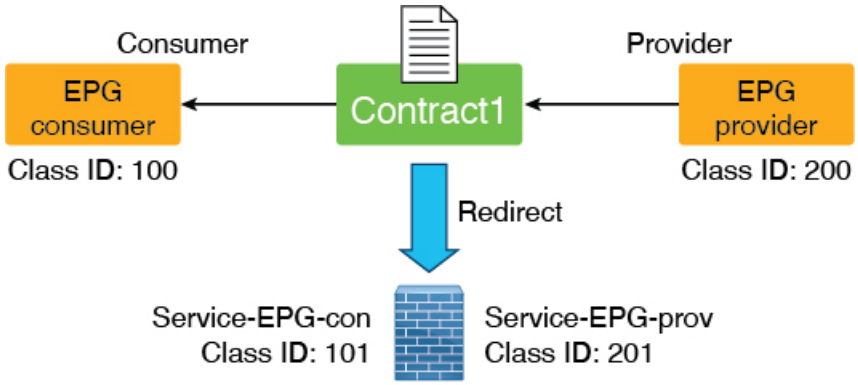
リリース 5.2(4) で導入されたサービス EPG セレクタ オプションを使用せずに必要な構成を有効にするには、[**直接接続（Direct Connect）**] オプションを使用できます。次の図は、[**直接接続（Direct Connect）**] オプションがデフォルト（無効）設定の構成例を示しています。



Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	100	Redirect
101	100	permit

504130

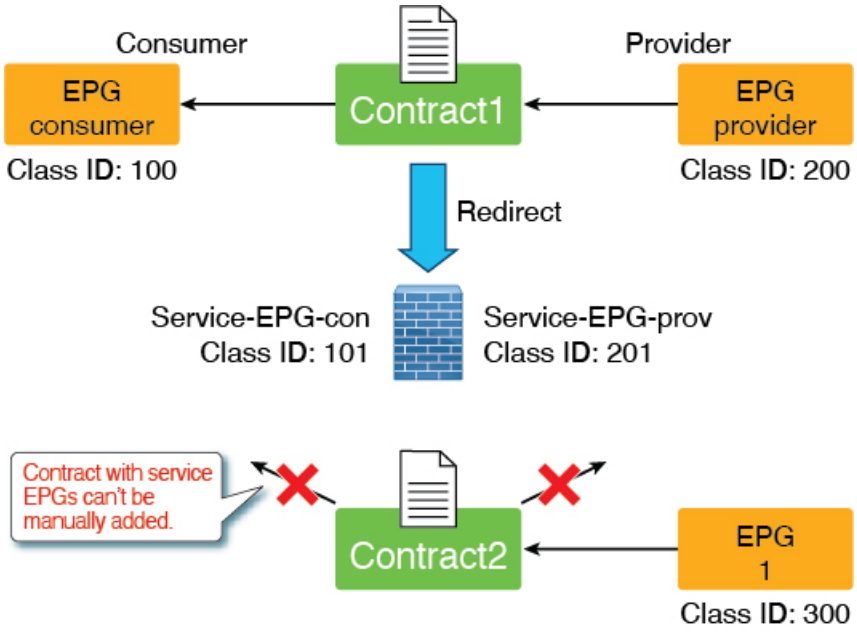
次の図は、[**直接接続（Direct Connect）**] オプションが有効になっている例を示しています。サービス EPG からコンシューマーまたはプロバイダー EPG へのトラフィックに許可ルールが追加されます。



Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	201	permit
200	100	Redirect
101	100	permit
100	101	permit

504131

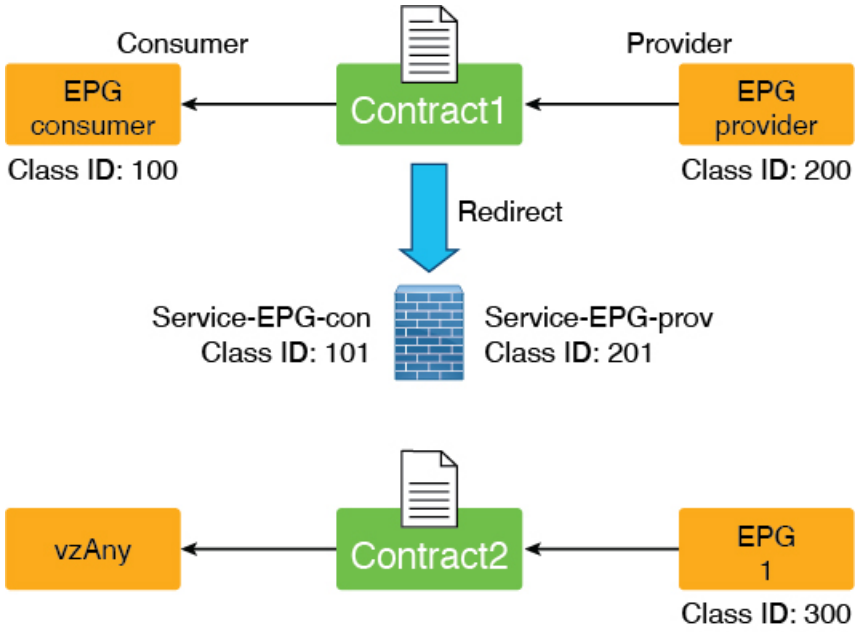
ただし、[**直接接続（Direct Connect**）] オプションが有効になっていても、コンシューマーまたはプロバイダー EPG ではない EPG にはサービス EPG の許可ルールがなく、コントラクトを手動で追加することはできません。



Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	201	permit
200	100	Redirect
101	100	permit
100	101	permit

504132

この制限を回避する方法の 1 つとして、次の図に示すように、サービス EPG が vzAny 構成の一部である vzAny コントラクトを構成する方法があります。

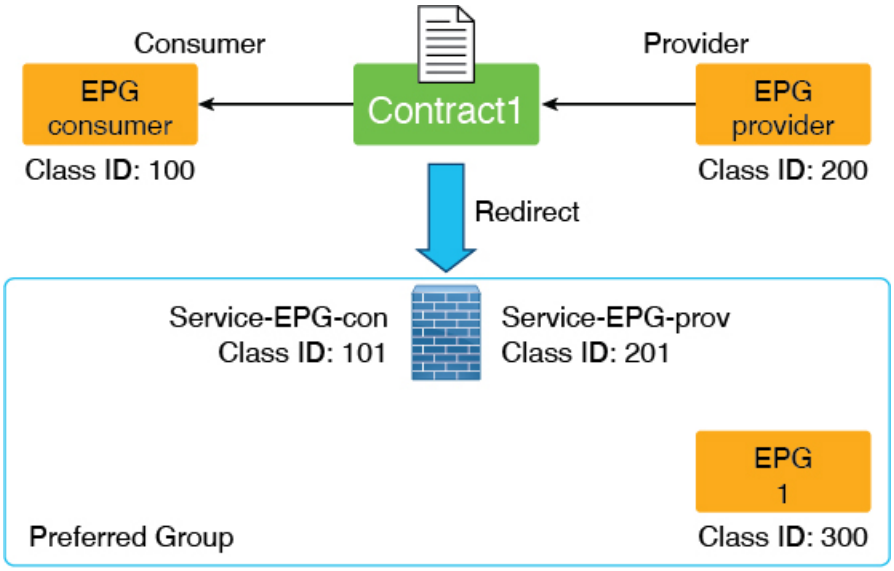


Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	100	Redirect
101	100	permit
0	300	permit
300	0	permit

504133

ただし、この回避策で考慮する事項として、EPG（前の例のクラス ID 300）も VRF 内の他の EPG と通信できることがあります。

2 番目に考えられる回避策は、次の図に示すように優先グループを構成することです。



Source EPG	Destination EPG	action
100	200	Redirect
201	200	permit
200	100	Redirect
101	100	permit
0	0	permit
0	100	deny
100	0	deny
0	200	deny
200	0	deny

504134

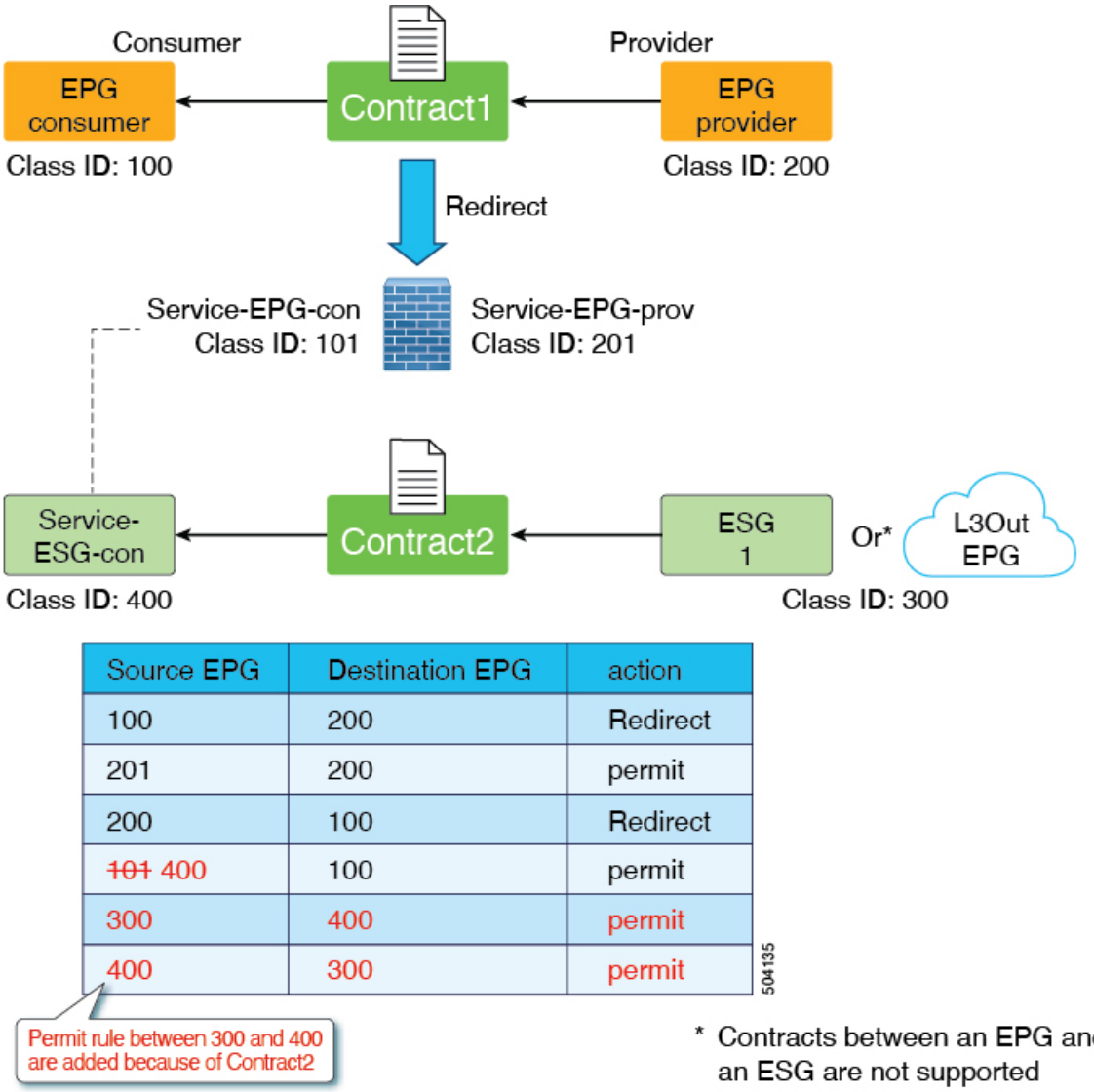
ただし、この 2 番目の回避策で考慮する事項として、優先グループ内の他の EPG がコントラクトなしで相互に通信できてしまうことがあります。また、より多くの TCAM リソースを消費する可能性もあります。

状況に対し、どちらの回避策も有効なソリューションではない場合、次のセクションで説明するように、リリース 5.2(4) 以降で利用可能なサービス EPG セレクタオプションを使用できます。

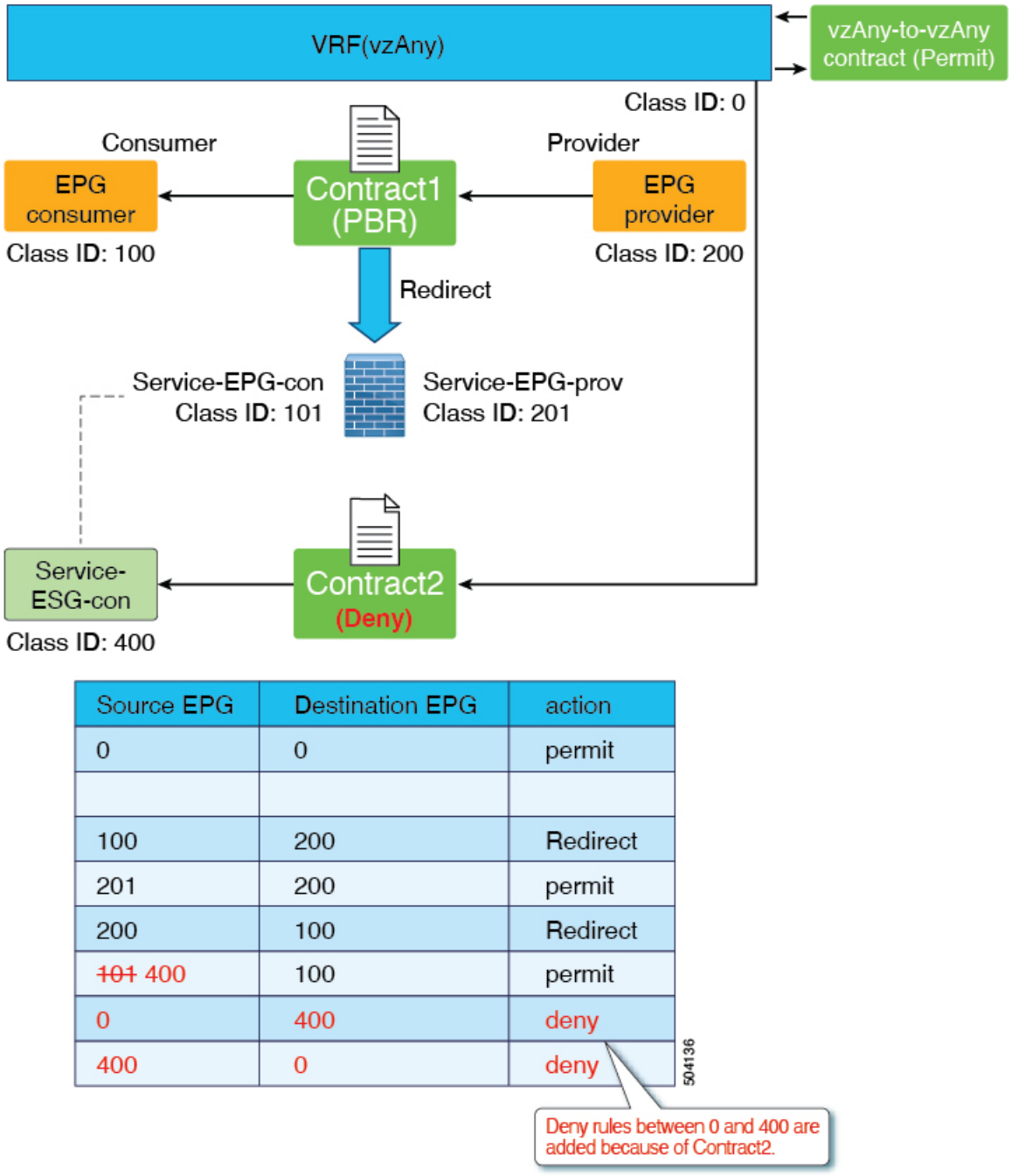
サービス EPG セレクタを使用した構成例

リリース 5.2(4) 以降で利用可能になったサービス EPG セレクタを使用すると、サービス EPG（`LifCtx`）を表すサービスデバイスコネクタを ESG にマッピングできます。これにより、ESG とのコントラクトを追加できます。さらに、サービス EPG セレクタを使用すると、サービス EPG に関連するゾーン分割ルールが継承されます。

サービス EPG セレクタを使用した構成例を次の図に示します。



サービス EPG セレクタ機能を使用するもう 1 つの方法は、vzAny-to-vzAny 許可コントラクトでサービスデバイスインターフェイスを除外することです。このシナリオでは、vzAny-to-vzAny を使用して VRF 内のすべてのトラフィックを許可しますが、次の図に示すように、サービス デバイス インターフェイスとの通信も禁止します。



ESG およびサービス EPG のサポートされている場所とサポートされていない場所

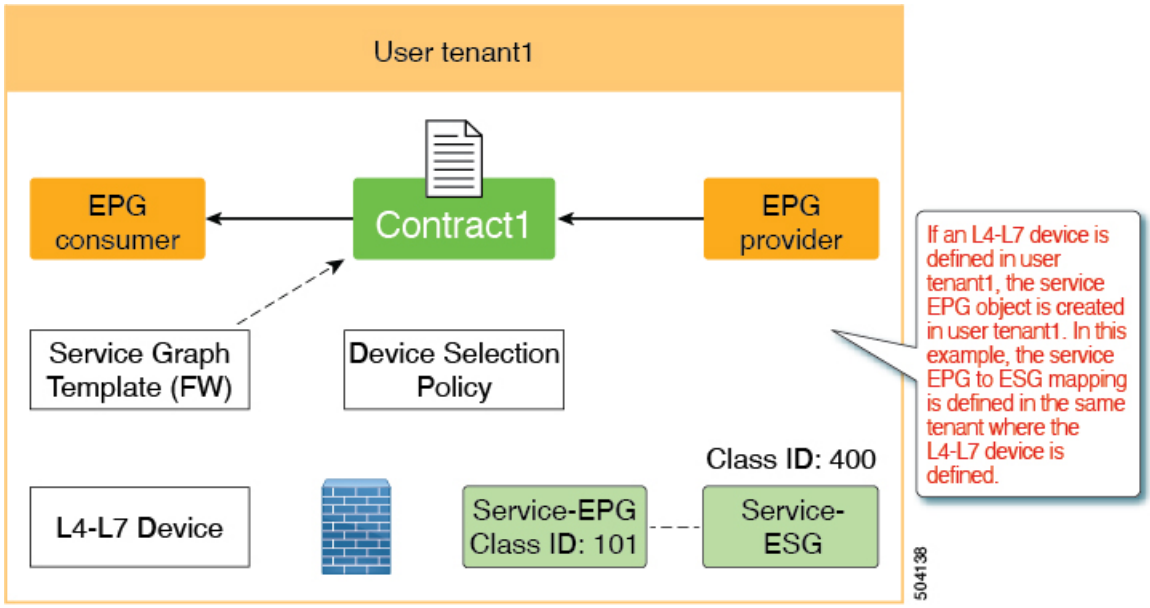
このセクションでは、ESG およびサービス EPG のサポートされているロケーションとサポートされていないロケーションに関する情報を提供します。

このセクションは、管理者が ESG からレイヤ 4 からレイヤ 7 デバイスに向けられたトラフィックを許可または拒否する必要がある設計にのみ関連します。レイヤ 4 からレイヤ 7 デバイスにリダイレクトされるトラフィックは、このカテゴリに属さず、このセクションで説明されてい

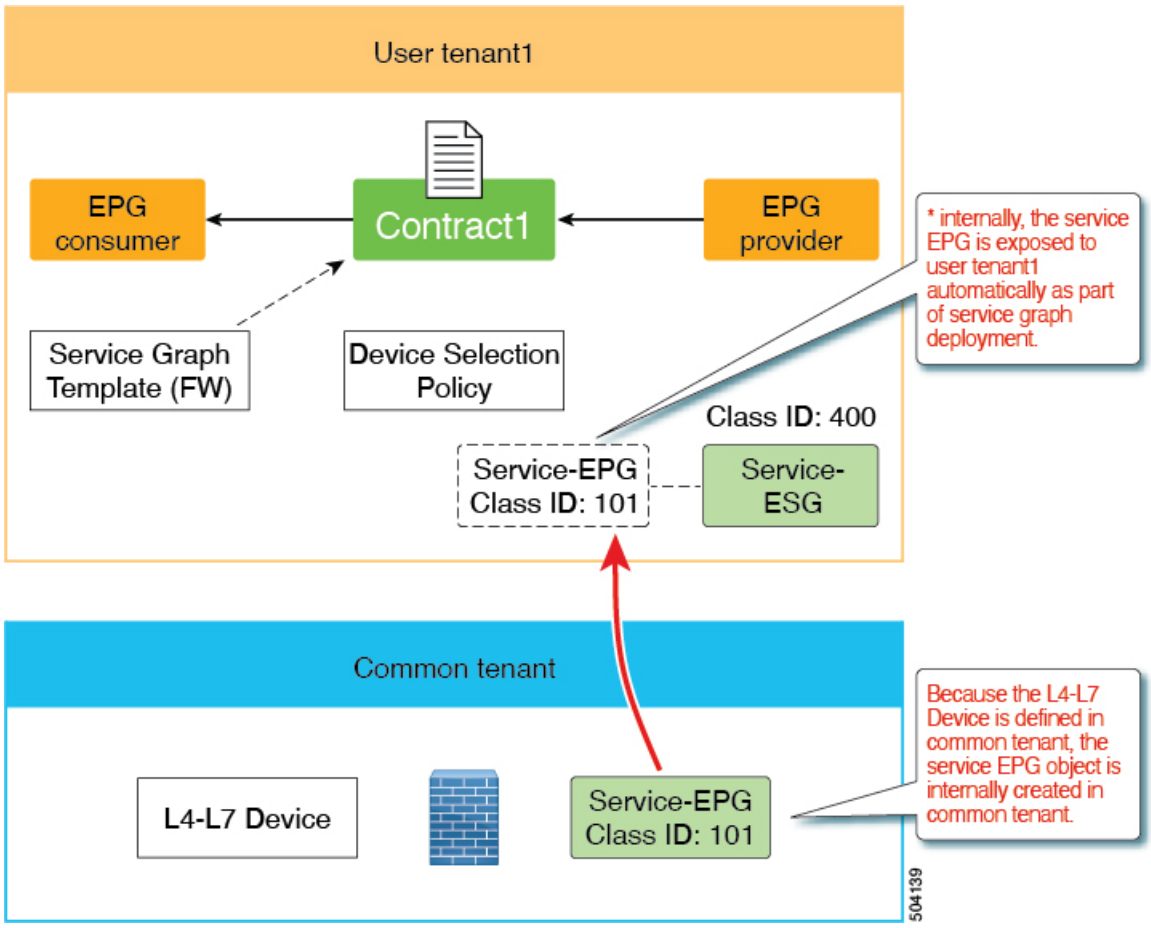
る制限の対象ではありません。これは、リダイレクトされたトラフィックの宛先 IP アドレスがエンドポイントであり、レイヤ 4 からレイヤ 7 のデバイス IP アドレスではないためです。

（注） サービス EPG は、レイヤ 4 ～ レイヤ 7 デバイスが定義されているテナントで内部的に作成されます。

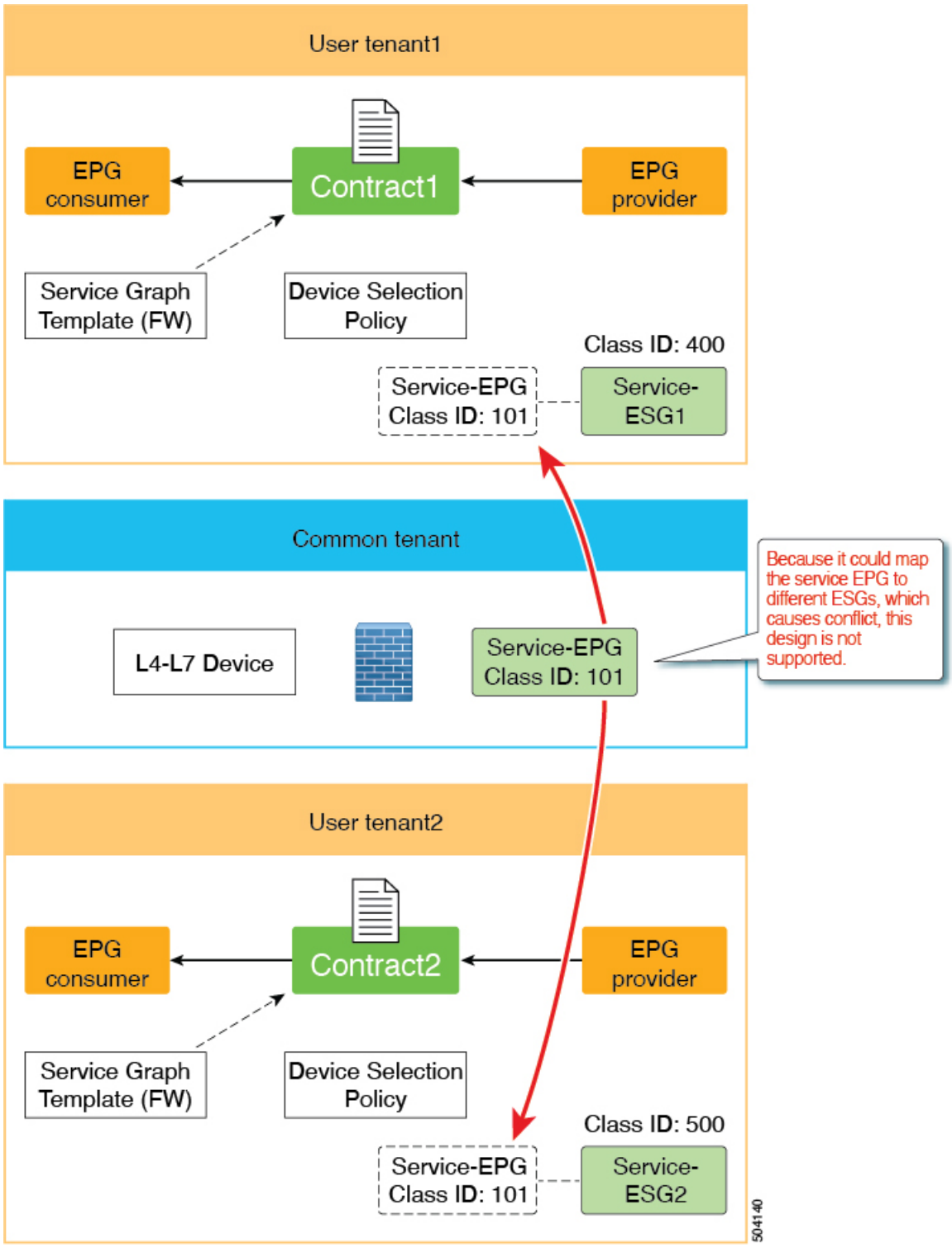
- **サポート**：レイヤ 4 ～ レイヤ 7 デバイスとサービス EPG から ESG へのマッピングは、同じテナントで定義されます。



- **サポート**：レイヤ 4 ～ レイヤ 7 デバイスは共通テナントにあり、サービス EPG から ESG へのマッピングはユーザーテナントで定義されます。下の図の例では、共通テナントのレイヤ 4 ～ レイヤ 7 デバイスが、サービスグラフが構成されているユーザーテナント `tenant1` にエクスポートされます。



- **サポート対象外**：レイヤ4～レイヤ7デバイスは共通のテナントにあり、複数のテナント間で共有されます。つまり、サービス EPG から ESG へのマッピングは複数のユーザーテナントで実行されます。

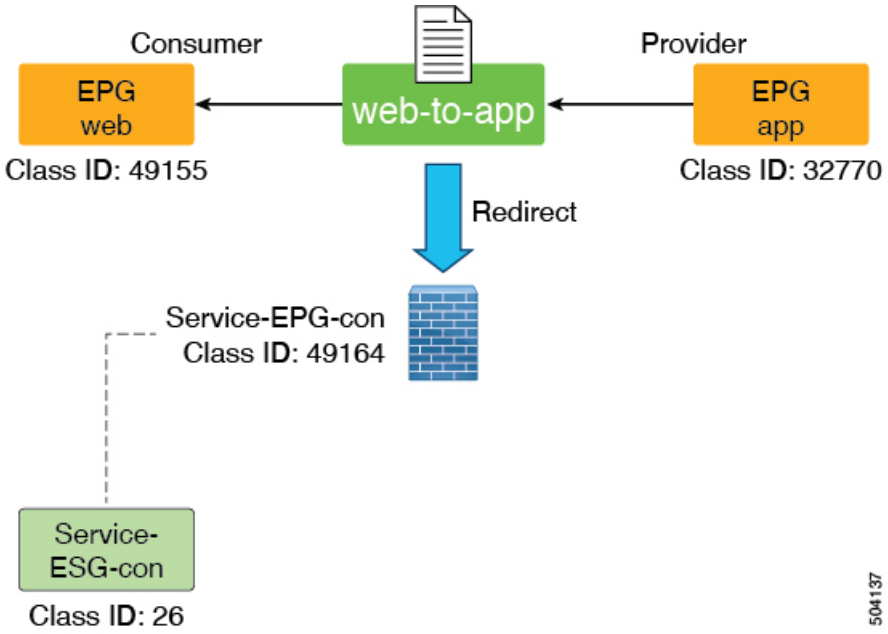

User tenant1
EPG consumer
Contract1
EPG provider
Service Graph Template (FW)
Device Selection Policy
Class ID: 400
Service-EPG Class ID: 101
Service-ESG1
Common tenant
L4-L7 Device
Service-EPG Class ID: 101
Because it could map the service EPG to different ESGs, which causes conflict, this design is not supported.
User tenant2
EPG consumer
Contract2
EPG provider
Service Graph Template (FW)
Device Selection Policy
Class ID: 500
Service-EPG Class ID: 101
Service-ESG2
504140

サービス EPG セレクタの注意事項と制限事項

次に、リリース 5.2(4) で導入されたサービス EPG セレクタ機能の注意事項と制限事項を示します。

- サービス EPG に関連するゾーン分割ルールは継承されますが、サービス EPG のクラス ID は、グローバルクラス ID を使用する ESG にマッピングされるため、グローバルクラス ID に変更されます。サービス EPG のクラス ID が変更されると、トラフィック損失が発生します。
- 同じブリッジドメインを使用する同じデバイス内のすべてのサービスデバイスコネクタ（`LifCTx`）は、同じ ESG にマッピングする必要があります。

  たとえば、次の図に示すように、PBR サービスグラフを使用してワンアームモードのファイアウォールを構成したとします。



  この例では、コンシューマーコネクタとプロバイダーコネクタは同じブリッジドメインにあり、同じサービス EPG を使用しています。この場合、両方のコネクタを同じ ESG にマップする必要があります。同じサービス EPG を使用するコネクタが同じ ESG にマッピングされていない場合、障害が発生し、サービスグラフの展開は失敗します。

  複数のサービスグラフの展開にサービスデバイスインターフェイスを再利用できることに注意してください。

- サービス EPG と ESG は同じ VRF にある必要があります。
- 現時点では、NDO は ESG をサポートしていないため、この機能は NDO ではサポートされていません。
- サポートは、ブリッジドメインの PBR 宛先を持つレイヤ 3 PBR でのみ使用できます。

- L3Out の PBR 宛先はサポートされていません（コントラクトは L3Out EPG により手動で構成できます）
- レイヤ 1/レイヤ 2 PBR はサポートされていません (レイヤ 1/レイヤ 2 デバイスインターフェイスはサーバーと直接通信することを想定していません)

IP ベース セレクターによるレイヤー 2 トラフィック制限

ESG ではさまざまな分類方法があるため、IP アドレスと MAC アドレスの分類の相違点を理解することが重要です。この相違点は、基本的にマイクロセグメント（uSeg）EPG 基準と同じです。

パケットがスイッチによってルーティングされる場合、転送ルックアップは IP アドレスに基づいて行われます。パケットがスイッチによってスイッチングされる場合、パケットに IP ヘッダーがある場合でも、転送ルックアップは MAC アドレスに基づいて行われます。同様に、パケットがスイッチによってルーティングされる場合、コントラクトルックアップは IP アドレスに基づいています。パケットがスイッチによって切り替わる場合、パケットに IP ヘッダーがある場合でも、コントラクトルックアップは MAC アドレスに基づいています。この動作は、以下のように ESG に基づくコントラクトの適用に影響します。

IP ベースのセレクタ（IP サブネットセレクタ、BD サブネットまたは IP エンドポイント タグオブジェクトのポリシータグに一致するタグセレクタなど）は、IP アドレスのみを分類します。このような分類は、スイッチングトラフィックには適用されません。一方、他のセレクタは MAC アドレスを分類し、そのような分類はスイッチングトラフィックとルーティングトラフィックの両方に有効です。これは、別の IP ベースのセレクタによってオーバーライドされない限り、MAC ベースのセレクタが MAC アドレスに関連付けられた IP アドレスにも適用されることを意味します。この動作は、次の 3 つのシナリオで示されています。

これらのシナリオでは、エンドポイント EP_A は EPG_A のメンバーであり、最初はどの ESG にも属していません。EP_A の MAC アドレスは MAC_A で、その IP アドレスは IP_A です。

```
Scenario 1:
    MAC_A is matched by a selector of ESG_1
    IP_A is _not_ matched by any ESG
  Result:
    Both MAC_A and IP_A are classified to ESG_1

Scenario 2:
    MAC_A is matched by a selector of ESG_1
    IP_A is matched by a selector of ESG_2
  Result:
    MAC_A is classified to ESG_1
    IP_A is classified to ESG_2

Scenario 3:
    MAC_A is _not_ matched by any ESG
    IP_A is matched by a selector of ESG_2
  Result:
    MAC_A is _not_ classified to any ESG, and still belongs to EPG_A.
    IP_A is classified to ESG_2
```

この動作により、トラフィックの送信元と宛先の IP アドレスが異なる ESG に属している場合でも、IP ベースのセレクタが使用されている場合、スイッチングトラフィック（レイヤ2 トラフィック）が ESG コントラクトをバイパスする可能性があります。IP ベースのセレクタでこの問題を回避するには、ACI のプロキシ ARP 機能を使用して、送信元と接続先の IP アドレスが同じサブネットにある場合でも、すべてのトラフィックが ACI スイッチで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必要があります。この目的でプロキシ ARP を使用するには、次の 3 つのオプションがあります。

- ESG エンドポイントに VLAN からインターフェイスへのバインドを提供するすべての EPG で、プロキシ ARP とともに EPG 内分離を有効にします。
- ESG エンドポイントに VLAN からインターフェイスへのバインドを提供するすべての EPG で、共通のデフォルトコントラクトなどのすべて許可（permit-all）フィルタを使用して、EPG 内コントラクトを有効にします。EPG 内コントラクトにより、プロキシ ARP が自動的に有効になります。すべて許可する（permit-all） フィルタである理由は、どの ESG にも分類されていないエンドポイントが、同じ EPG 内で相互に通信できるようにするためです。ESG にまだ分類されていないエンドポイントのデフォルトの動作として、任意のフィルタを使用できます。
- VMM 統合が使用されている場合に、ESG エンドポイントに VLAN からインターフェイスへのバインドを提供する EPG に VMM ドメインを関連付ける際に、[**マイクロセグメンテーションを許可（Allow Micro-Segmentation**）] オプションを有効にします。このオプションは、プロキシ ARP を自動的に有効にします。

同じサブネット（または VLAN）内のエンドポイントが異なる ESG に分類されるレイヤ 2 トラフィックの場合、IP ベースのセレクタによるレイヤ2 トラフィックの制限に関係なく、プライベート VLAN 構成が必要になる場合があります。エンドポイントと ACI スイッチの間に非 ACI スイッチがある場合は、プライベート VLAN 構成が必要になる場合があります。これは、ACI スイッチが ESG に基づいてコントラクトを実施できるようになる前に、非 ACI スイッチがトラフィックをスイッチングする可能性があるためです。

セレクターの優先順位

セレクタータイプを選択するときは、トラフィックを切り替えるかルーティングするかを考慮してください。以下の表は、トラフィック タイプごとのセレクターの優先順位を示しています。

表 *1:* スイッチング トラフィックの優先順位

優先順位	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 セレクター（エンドポイント VMM MAC タグ）
3	EPG セレクター

表 *2:* ルーティング トラフィックの優先順位

優先順位	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 セレクター（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 セレクター（エンドポイント VMM MAC タグ）
5	EPG セレクター

オブジェクトが同じまたは異なるポリシー タグを介して複数のタグ セレクターで一致した場合、そのオブジェクトは最初に一致したタグ セレクターに関連付けられます。後続のタグ セレクターは無視されます。タグセレクターが以前にオブジェクトに一致していないときに、オブジェクトが複数のタグセレクターによって一致した場合、競合の一致が解決されるまでタグセレクターは有効になりません。障害は、複数のタグ セレクターによって一致する ESG およびオブジェクトの下で発生します。

コントラクト

コントラクトは、アクセスコントロールリスト（ACL）に相当する Cisco ACI です。ESG は、コントラクト規則に従う場合に限り、他の ESG と通信できます。管理者は契約を使用して、許可されているプロトコルとポートを含む ESG 間をパス可能なトラフィックの種類を選択します。ESG は、コントラクトのプロバイダー、コンシューマー、またはプロバイダーとコンシューマーの両方になることができ、複数のコントラクトを同時に使用できます。複数の ESG が優先グループに属する他の ESG と自由に通話できるように、ESG は優先グループに属することもできます。

サポートされているコントラクト関係：

1. ESG ⇔ ESG
2. ESG ⇔ L3Out EPG
3. ESG ⇔ インバンド EPG
4. ESG ⇔ vzAny

ESG と EPG（または uSeg EPG）の間のコントラクトはサポートされていません。ESG のエンドポイントが EPG の他のエンドポイントと通信する必要がある場合、他のエンドポイントを最初に ESG に移行する必要があります。 vzAny または優先グループは、移行中に代替として

使用できます。コントラクト継承、ESG内コントラクト、ESG内分離など、uSeg EPGでサポートされるその他のコントラクト関連機能もESGでサポートされます。例外は、ESGでサポートされていない禁止コントラクトです。

vzAny

ESG間の特定のコントラクトを使用する代わりに、vzAnyと呼ばれるConstructを使用してESG間のトラフィックを許可することもできます。

vzAnyは、特定のVRFインスタンス内のすべてのESGおよびEPGを表します。これには、VRFインスタンス内のL3Out外部EPG（`l3extInstP`）も含まれます。vzAny Constructは、そのVRFインスタンス内のすべてのEPGとESGを簡単に参照できるようにします。vzAny参照は、VRFインスタンス内のすべてのEPGおよびESGの単一のコントラクト構成を可能にすることで管理を容易にし、各EPGまたはESGに個別にではなく、この1つのグループにコントラクトを適用することにより、ハードウェアリソースの消費を最適化します。

図 *4 : vzAny* は、同じ *VRF* インスタンス内のすべての *EPG* と *ESG* を表す省略形です。

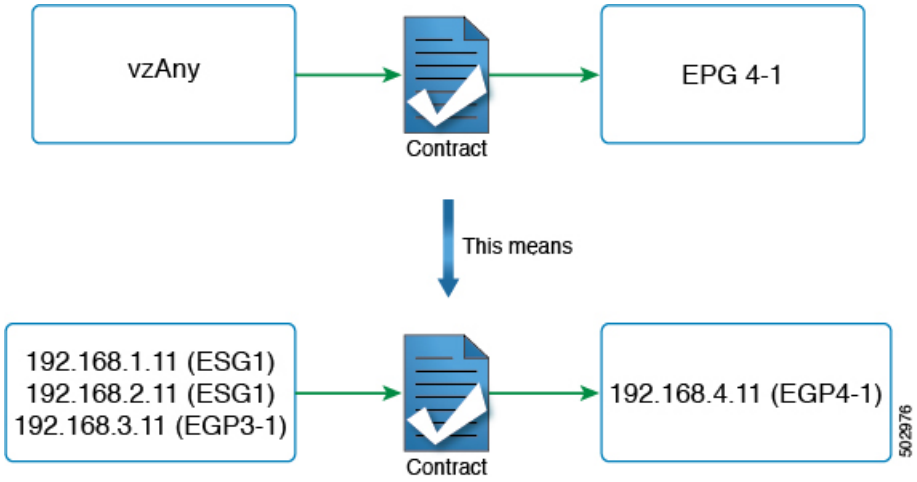


図4に例を示します。図2のトポロジで、管理者がvzAnyとEPG 4-1の間のコントラクトを構成した場合、エンドポイント192.168.1.11、192.168.2.11（ESG1）、および192.168.3.11（EPG3-1）は192.168.4.11（EPG4-1）と通信できます。

これは、ESG1とEPG3-1が同じセキュリティゾーンに属しており、192.168.11（または192.168.2.11）がコントラクトなしで192.168.3.11と通信できるという意味ではありません。必要な構成が、ESG、EPG、L3Out EPGなどに関係なく、VRFインスタンス内の任意の通信を許可することである場合、ユーザーは、VRFインスタンスで**ポリシーの適用**（非強制）を無効にする代わりに、すべてのトラフィックを許可するコントラクトを提供および消費するようにvzAnyを構成できます。

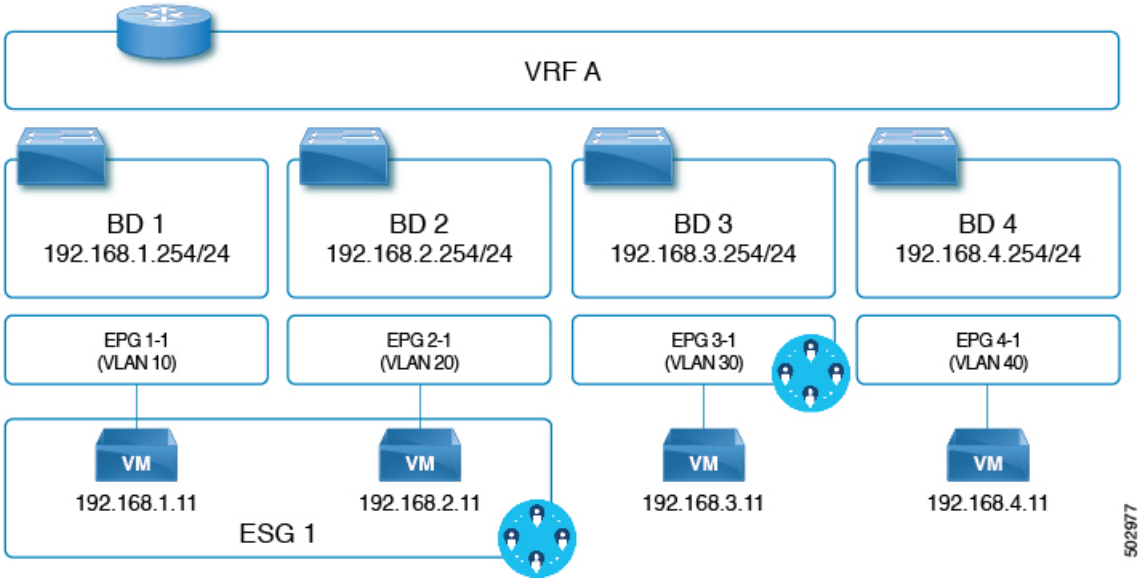
つまり、vzAny Constructによって、EPGと同様にESGがコントラクトを使用してVRFインスタンス内の誰とでも通信できるようにするために、コントラクトを提供および（または）消費するために使用できます。ESGとEPG間のコントラクトは許可されていませんが、vzAnyコントラクトを使用してESGとEPG間のトラフィックを許可できます。

優先グループ

優先グループは、ESG間で明示的な契約を使用したり、vzAny契約を使用したりする代わりに使用できます。ユーザーは、優先グループを設定して、VRF インスタンス内の ESG 間の通信を有効にすることもできます。優先グループ内のエンドポイントは、互いに自由に通信できます。

ユーザーは、優先グループを使用して、ESGからEPGへの通信を有効にすることもできます。これは、EPG ベース セキュリティ設定から ESG ベースのセキュリティ設定への移行に役立ちます。

図 *5*: 同じ優先グループの *ESG1* および *EPG3-1* 部分の例。



上の図の例では、ESG1 と EPG3-1 が VRF A の優先グループの一部になるように設定されており、次の通信が許可されています。

1. ESG 1 と EPG 3-1 は、両方が優先グループに含まれているため、相互に通信できます。
2. ESG 1 と EPG 4-1 は、次の理由で相互に通信できません。
   - EPG 4-1 は優先グループに含まれません。
   - EPG と ESG 間の契約はサポートされていません。

優先グループの設定については、『Cisco APIC 基本設定ガイド』を参照してください。

ESG 共有サービス（ESG VRF ルート リーク）

エンドポイントが別の VRF によって共有されるサービスを必要とする場合、通信を行うために必要なことが 2 つあります。まず、ルーティングの到達可能性です。2 つ目はセキュリティ

許可です。EPG では、これら 2 つは EPG サブネットや契約などの 1 セットの設定で密接に結合されています。ESG では、これら 2 つは 2 つの異なる設定で分離されています。

1. ESG 契約の設定とは独立した、VRF レベルでのルート リークの設定。
2. ESG 間の契約の設定。

これら 2 つの設定が完全に分離されているため、EPG で行う必要があるように、ESG の下にサブネットまたはサブネットのサブセットを設定する必要はありません。

次のセクションでは、ブリッジ ドメイン サブネットおよび外部ルーターから学習した外部プレフィックスのルート リークを設定する方法について説明します。ルート リークの設定が完了したら、2 つの ESG 間、または ESG と L3Out EPG 間の契約を設定して、通信を許可できます。グローバルなど、VRFより大きい範囲の契約を使用する必要があります。

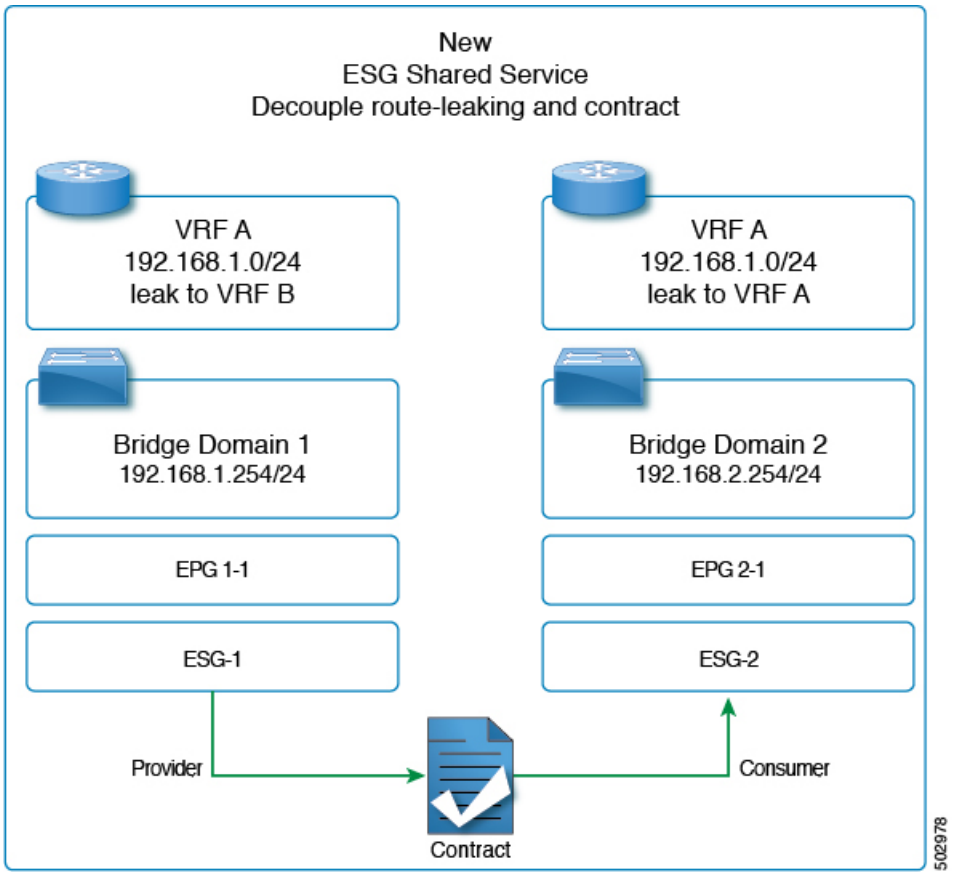
（注） VRF レベルでのルート リーク設定は、ESG でのみサポートされます。

内部ブリッジドメインサブネットのルートリーク

このセクションでは、ESG エンドポイントが属するブリッジドメインサブネットの VRF インスタンス間のルートリークを構成する方法について説明します。これは、ESG を使用しない場合に EPG レベルで実行されるのではなく、リークするサブネットと、VRF レベルで送信元 VRF インスタンスのターゲット VRF インスタンスを指定するだけで実行します。ルートリーク構成で入力するサブネットは、ブリッジドメインサブネットと一致するか、構成されたブリッジドメインサブネットのサブセットである必要があります。この構成でリークされるルートは、指定されたサブネットマスクを持つサブネットのみです。1 つの構成で複数のブリッジドメインサブネットをリークするサブネットの範囲を指定することはできません。

（注） VRF ルートリーク構成で構成するサブネットは、EPG で使用されるサブネットと一致させることもできます。これは、移行する場合に役立ちます。

図 *6 : ESG* によるルートリーク



上の図は、管理者が ESG1 と ESG2 の 2 つの ESG を構成した、2 つの VRF インスタンス（VRF A と VRF B）間の VRF リークの例を示しています。

（トラフィックを許可するための）ESG1 と ESG2 間のコントラクトに加えて、管理者はセクション「GUI を使用した内部ブリッジ ドメイン サブネットのルート リークの設定」で説明されているように、VRF インスタンスでルートリークを構成する必要があります。

ブリッジドメインサブネット範囲の構成 （[**外部でアドバタイズ（Advertised Externally）**]、[**VRF 間で共有（Shared between VRFs）**]）は、ESG の VRF レベルのルートリークでは必要ありません。リークされたブリッジドメインサブネットをターゲット VRF インスタンスの L3Out によってアドバタイズする必要がある場合は、VRF レベルのルートリーク構成で [**L3Out アドバタイズを許可（Allow L3Out Advertisement）**] を [**はい（True）**] に設定できます。 VRF レベルのルートリークで指定されたターゲット VRF インスタンスにサブネットをリークする場合、ブリッジドメインの下のサブネット範囲は無視され、VRF レベルのルートリークの構成が優先されることに注意してください。ブリッジドメインの下にあるこれらの範囲は、同じ VRF インスタンス内の L3Out からサブネットのアドバタイズ、EPG コントラクトによる従来の構成を介して別の VRF インスタンスへのルートリーク、またはその両方など、同時に他の構成でも引き続き優先されます。

外部プレフィックスのルートリーク

VRF の L3Out から別の VRF の ESG へのトラフィックを許可するためのルートリークの構成は、EPG の共有 L3Out と区別するために **ESG 共有 L3Out** と呼ばれます。

ESG 通信の L3Out から学習したルートをリークするには、管理者は VRF レベルで外部プレフィックスのルートリークを構成する必要があります。これは、IP プレフィックスリスト スタイルの構成を使用して行われます。ユーザーは、通常ルータの IP プレフィックスリストと同様に、「le」（以下）または「ge」（以上）を使用して、特定のプレフィックスを構成するか、プレフィックスの範囲を指定できます。ブリッジドメインサブネットとは異なり、外部ルートは動的に学習され、予測できないことが多いため、リークされたプレフィックスが実際のルート以下でなければならないという制限はありません。制限がないため、リークされた外部プレフィックスは、1 つの構成で複数のプレフィックスをリークする範囲を指定できます。設定では、ターゲット VRF も指定する必要があります。

設定の詳細については、『GUI を使用して外部プレフィックスのルートリークを構成する』を参照してください。

ESG 共有 L3Out 構成の場合、VRF でルートリークを構成し、L3Out EPG とのコントラクトを適用するとともに、どのプレフィックスがどの L3Out EPG に属するかを定義する必要があります。どのプレフィックスがどの L3Out EPG に属するかを指定するには、**外部 EPG の外部サブネット**および**共有セキュリティインポート サブネット**範囲を使用して L3Out サブネットを構成する必要があります。

レイヤ 4 ～ レイヤ 7 サービス

EPG で使用できるすべてのレイヤ 4 ～ レイヤ 7 サービス グラフ機能は、ESG でサポートされます。

（注） このメモは、高度なユーザー情報の実装の詳細です。ESG 間のコントラクトにサービス グラフが適用されている場合、Cisco Application Policy Infrastructure Controller (APIC) では、レイヤ 4 ～ レイヤ 7 サービスデバイスが適用される非表示サービス EPG を、 Cisco APIC が EPG 間のサービスグラフに行うのと同じように自動的に作成します。EPG 間のサービス グラフとは異なり、ESG の場合、隠しサービス EPG はグローバル pcTag を取得します。

Cisco APIC リリース 5.0(1) 以降のリリースでは、vzAny-to-vzAny コントラクトでレイヤ 4 ～ レイヤ 7 サービス展開用に作成されるすべての新しいサービス EPG は、グローバル pcTag を取得します。

レイヤ 4 ～ レイヤ 7 サービス展開の詳細については、『Cisco APIC レイヤ 4 ～ レイヤ 7 サービス導入ガイド』を参照してください。

運用ツール

キャパシティ ダッシュボード

[Capacity Dashboard] タブを使用して、重要なファブリック リソースのしきい値の概要を把握できます。これにより、承認されるスケーラビリティ制限にどの程度まで近づいているかを即座に確認できます。リーフ ノードごとの使用量も表示されるため、どのリーフ ノードがリソース制約に達しているかをすぐに確認できます。

1. [容量ダッシュボード（Capacity Dashboard）] トラブルシューティング ツールを起動するには、メニュー バーで、**[操作（Operations）][容量ダッシュボード（Capacity Dashboard）]** の順に選択します。
2. **[容量ダッシュボード（Capacity Dashboard）]** ページで、ファブリック リソースの **[ファブリック容量（Fabric Capacity）]** を選択します。**[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** タイルと **[グローバル pcTag（Global pcTag）]** タイルまでスクロール ダウンして、使用可能なリソースを確認します。
3. **[容量ダッシュボード（Capacity Dashboard）]** ページで、リーフの使用状況として **[リーフ容量（Leaf Capacity）]** を選択します。エンドポイント セキュリティ グループのリソース使用量の詳細については、**[ESG]** タブを確認してください。

エンドポイント トラッカー

[**エンドポイントトラッカー（Endpoint Tracker**）] タブを使用して、ファブリックに適用されたエンドポイントの IP アドレスまたは MAC アドレスを入力すると、このエンドポイントのロケーション、エンドポイントが属するエンドポイントグループ、使用されている VLAN カプセル化、このエンドポイントで移行（フラップ）が発生しているかどうかをすばやく確認できます。

1. メニュー バーで、**[操作（Operations）]** > **[EP トラッカー（EP Tracker）]** の順にクリックして、エンドポイント トラッカーのトラブルシューティング ツールを起動します。
2. [End Point Search] フィールドに、エンドポイントの IP アドレスまたは MAC アドレスを入力し、[Search] をクリックします。
3. 表示された後にエンドポイントをクリックします。

エンドポイントトラッカー ツールでは、イベント中の IP アドレス、MAC アドレス、所有するエンドポイントグループ、アクション（適用または解除）、物理ノード、インターフェイス、および VLAN カプセル化とともに、各状態遷移の日時が表示されます。

エンドポイント トラッカー ツールは、fvCEp と呼ばれるオブジェクトを使用して、ESG および EPG について、ファブリックで学習されたエンドポイントを見つけます。ESG に属するエンドポイントは 2 つの fvCEp オブジェクトで表されます。1 つは VLAN バインドを提供する

EPG 用で、もう 1 つはセキュリティを提供する ESG 用です。したがって、エンドポイントトラッカーツールは、ESG エンドポイントに使用すると、2 つのエントリが表示されます（EPG 用と ESG 用）。

制限事項

Cisco APIC リリース 5.0(1) の時点で、次の制限が適用されます。

- ESG と EPG 間の契約はサポートされていません。
- ESG 機能は Cisco ACI マルチサイトと統合されていません。マルチポッド、マルチティア、リモート リーフなどの他のトポロジがサポートされています。
- サポートされている ESG セレクターは IP アドレスです。MAC アドレス、VM タグ、またはその他の基準はまだサポートされていません。
- ESG 契約は、セレクターとして IP を使用するルーティング トラフィックにのみ適用できます。
- タブー契約は ESG ではサポートされていません。
- ESG 間の VRF 間サービス グラフはサポートされていません。
- ESG は、次の機能のソースまたは宛先としてサポートされていません。
  - オンデマンド原子カウンター
  - オンデマンド遅延測定
  - SPAN
- BD/EPG のエンドポイントが ESG に分類されている場合、BD または EPG レベルで設定された次の機能はサポートされません。
  - エンドポイント到達可能性（BD/EPG 上の静的ルート）
  - エニーキャスト サービス
  - Microsoft NLB
  - First Hop Security (FHS)
  - ホスト ベース ルーティング/ホスト ルート アドバタイズメント
- ESG 展開では、EX 以降の世代のリーフ ノードのみがサポートされます。
- IP がセレクターとして使用されている場合に、レイヤ 2 トラフィック（つまり、ルーティングされていないトラフィック）が ESG セキュリティをバイパスしないようにするには、ESG エンドポイントに VLAN からインターフェイスへのバインディングを提供するすべての EPG で、共通のデフォルト契約などすべてを許可するルールを使用して EPG 契約を有効にします。EPG 内のすべてのエンドポイントが ESG に分類されている場合は、代わりに、EPG 内の契約ではなく、EPG でプロキシ ARP を使用して EPG 内の分離を有効にす

ることができます。EPG が VMM DVS 統合にのみ使用される場合は、上記の他の 2 つのオプションの代わりに、**[マイクロセグメンテーションを許可する（Allow Micro-Segmentation）]** オプションを有効にすることもできます。いずれの機能も、ESG エンドポイント間のすべての通信がレイヤ 3 ルーティングを通過するようにします。

（注） このメモでは、すべてを許可するルールを使用した EPG 内契約と、プロキシ ARP を使用した EPG 内の分離の違いについて説明します。両方の機能の主な目的は同じで、プロキシ ARP を使用して、ACI リーフ スイッチ上ですべてのトラフィックをルートするようにすることです。EPG間契約が使用される場合、プロキシ ARP は EPG に対して暗黙的に有効になることに注意してください。違いは、ESGに属していないが、EPGで学習されたエンドポイントが2つ以上ある場合です。すべてを許可するルールを使用したEPG内契約では、このようなエンドポイントは、すべてを許可するルールにより同じ EPG 内で引き続き自由に通信できます。ただし、プロキシ ARP を使用した EPG 内分離では、そのようなエンドポイントは同じEPGにある場合でも通信できなくなります。

- 契約を ESG に追加する場合、ラベル設定はサポートされていません。

ESG 以降戦略

Cisco Application Policy Infrastructure Controller（APIC）リリース 5.2(1) 以降のリリースでは、EPG セレクタにより、エンドポイントセキュリティ グループ (ESG) が EPG からコントラクトを継承できるようになり、EPG から ESG への移行が簡素化されます。EPG セレクタによるコントラクトの継承により、エンドポイントは他のエンドポイントがまだ ESG に移行されていない場合でも、継承されたコントラクトを使用して他のエンドポイントとの通信を継続できるため、シームレスでフレキシブルな移行が可能になります。

以下の例では、次の図の EPG A1 の EPG から ESG への移行に焦点を当てます。EPG A1 からの現在の通信は、EPG B1、B2、および B3 とのコントラクト C1 を介して行われます。

図 *7: EPG* から *ESG* への移行を開始する準備をする

最初の手順は、ESG（次の図の ESG A1）を作成し、EPG セレクタを使用して EPG A1 をそれに一致させることです。

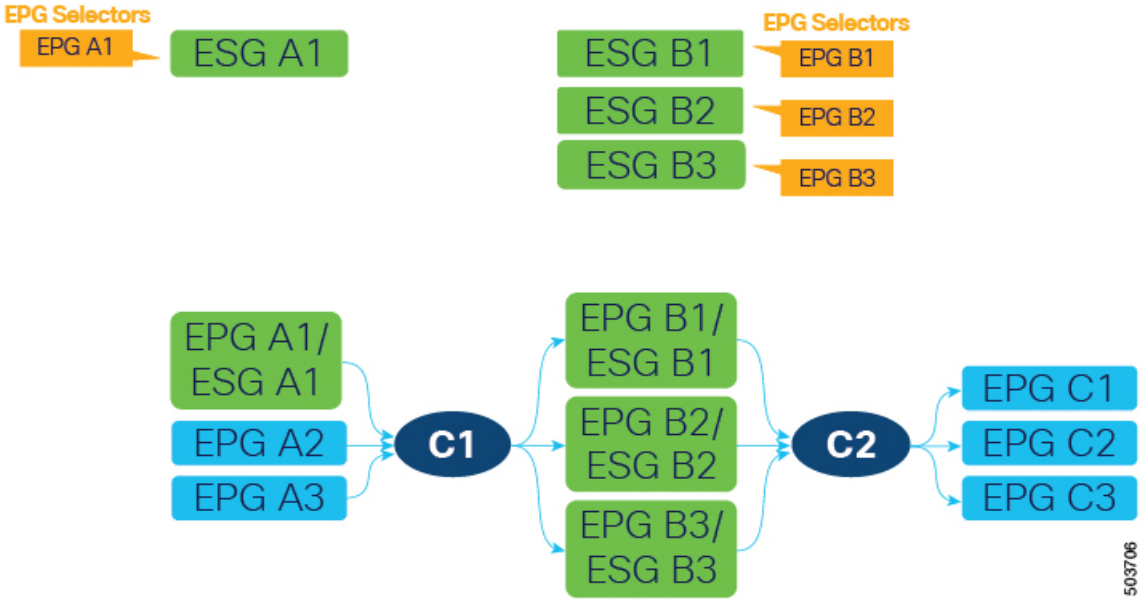
図 *8 : ESG* を作成し、最初の *EPG* を移行します

EPG A1 が ESG A1 に一致させた後、EPG A1 に属していたエンドポイントは ESG A1 に属し、EPG A1 によって提供されるコントラクト C1 は ESG A1 に継承されます。移行されたすべてのエンドポイントは、EPG がまだ ESG に移行されていなくても、EPG B1、B2、および B3 と引き続き通信できます。EPG セレクタによるコントラクトの継承がないと、Cisco Application Centric Infrastructure（ACI）は ESG と EPG 間のコントラクトが許可されないことに注意してください。ESG が EPG セレクタを介してコントラクトを継承する場合、EPG の元の pcTag は ESG の pcTag に置き換えられることに注意してください。この操作により、EPG のエンドポイントのトラフィックに一時的な小規模の中断が発生する場合があります。

この時点で、プロジェクトスケジュールに応じて、EPG A1 の移行を完了する代わりに、ESG A1 と他の ESG または L3Out 外部 EPG との間で新しいコントラクトを構成できます。ただし、すべてのセキュリティ構成は ESG によって管理される必要があるため、EPG A1 にこれ以上新しいコントラクトを追加することはできません。構成をシンプルに維持しやすくするために、できるだけ早く EPG から ESG への移行を完了することをお勧めします。EPG A1 がコントラクトの提供（または消費）を停止するまで、不完全な移行を通知する警告として障害 F3602 が発生します。

移行を続行するには、コントラクト C1 の反対側で EPG の ESG を作成します。この例では、EPG A1 がコントラクト C1 を提供しているため、それらの EPG（EPG B1、B2、および B3）がコントラクト C1 を消費しています。EPG セレクタを使用して、これらの EPG を新しい ESG（ESG B1、B2、および B3）に移行します。次の図の例では、各 EPG が ESG にマッピングされています。

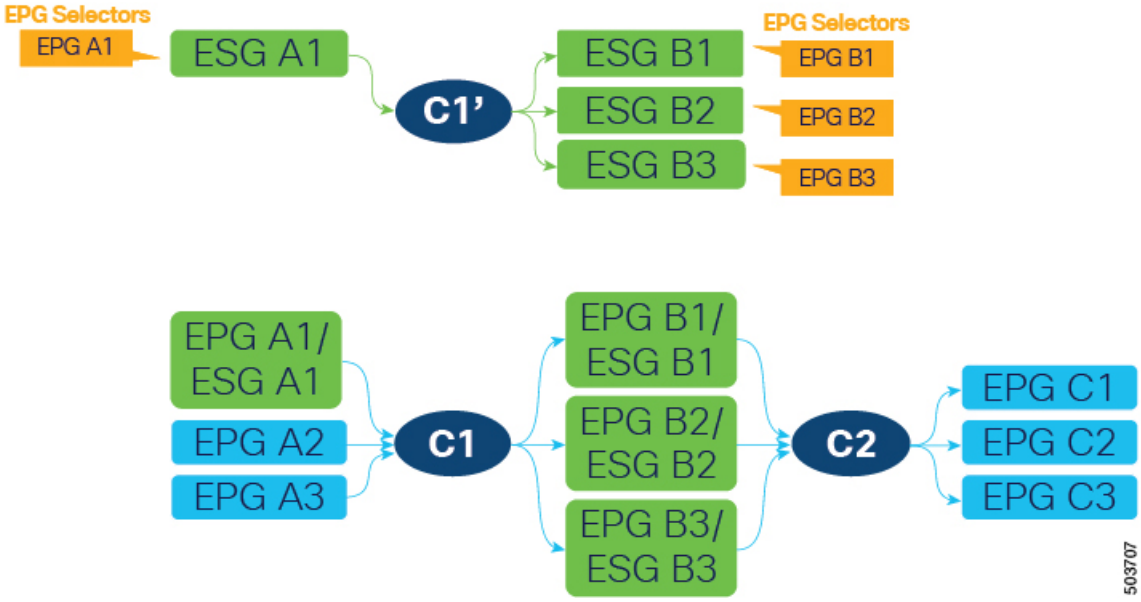
図 *9* : 追加の *ESG* の作成、*EPG* の移行



または、複数の EPG を 1 つの ESG に結合できます。たとえば、1 つの ESG を作成してから、同じ ESG 上の EPG B1 と B2 の両方に EPG セレクタを構成できます。

次に、コントラクト C1 と同じフィルタを使用して新しいコントラクト（次の図の C1'）を作成します。新しい ESG をプロバイダーおよびコンシューマーとして構成します。これは、EPG A1 からのコントラクト C1 の提供の停止を準備するため、EPG A1 の EPG から ESG への移行の最後の手順です。

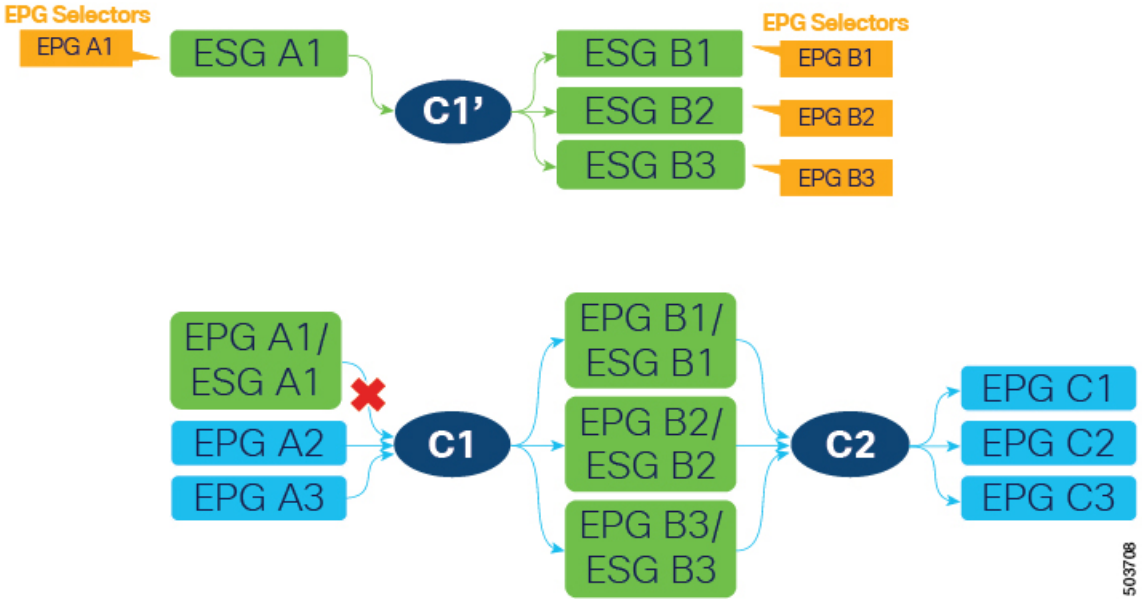
図 *10* : 新規契約を作成する



同じフィルタを持つコントラクトC1は、4つすべてのESG（A1、B1、B2、およびB3）によってすでに継承されているため、新しいコントラクト設定はハードウェアに新しいルールを展開せず、新しいコントラクトを作成することによって追加のポリシー TCAM が消費されることはありません。

ESG A1 には、ESG B1、B2、および B3 との C1 と同じ通信を許可するコントラクト C1' があります。この時点で、EPG A1 でのコントラクト C1 の提供を停止でき、次の図に示すように ESG A1 がすべてのセキュリティを処理できるようになります。

図 *11* : 古いコントラクトのプロバイダーとしての *EPG* を削除する



B1、B2、および B3 は、コントラクト C1 はまだ ESG に移行されていない EPG A2 および A3 によっても提供されるため、コントラクト C1 の消費をまだ停止できないことに注意してください。EPG A2 および A3 が ESG に移行され、コントラクト C1' を提供した後、すべての EPG（A2、A3、B1、B2、および B3）は、トラフィックを中断することなくコントラクト C1 の使用を停止できます。

EPG から ESG への移行を完了するには、EPG レベルのコントラクト C2 およびその他のコントラクトについても同じ手順に従います。

エンドポイント セキュリティ グループを設定する

GUI を使用してエンドポイントセキュリティ グループを作成する

Cisco APIC リリース 5.2(1) 以降のリリースでは、ESG セレクタはポリシータグ、EPG、IP サブネットにすることができます。以前のリリースでは、IP サブネットのみがサポートされています。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]**を選択します。

ステップ 3 [**エンドポイントセキュリティ グループ（Endpoint Security Groups**）] を右クリックし、[**エンドポイントセキュリティ グループの作成（Create Endpoint Security Group**）] を選択します。

ステップ 4 [**エンドポイントセキュリティ グループの作成（Create Endpoint Security Group**）] ダイアログボックスの [**手順 1（STEP 1**） > **ID（Identity**）] ページで、次の情報を入力します。

a) **名前（Name**）：ESG の名前を入力します。

b) （任意） **説明（Description**）：ESG の説明を入力します。

c) **VRF**：ESG に関連付けられる VRF を入力します。

d) **ESG 管理状態**：ESG をシャットダウンするには、[**管理者によるシャットダウン（Admin Shut**）] を選択します。デフォルトでは、[**ESG 管理状態（ESG Admin State**）] は [**Admin Up**] の値です。このフィールドは、5.2(3) リリースから追加されました。

e) [次へ（Next）] をクリックします。

[**エンドポイントセキュリティ グループの作成（Create Endpoint Security Group**）] ダイアログボックスの [**手順 2（STEP 2**） > **セレクタ（Selectors**）] ページが開きます。

（注） 次の手順では、ポリシータグ、EPG、および IP サブネットに基づいてセレクタを作成できます。または、[**次へ（Next**）]をクリックして、セレクタとタグを設定する （38 ページ）で説明するようにセレクタを後で構成することもできます。

ステップ 5 [**手順 2（STEP 2**） > **セレクタ（Selectors**）] ページで、ポリシータグをエンドポイントセレクタとして使用する場合は、**タグセレクタ**バーの [+] 記号をクリックします。

[タグ セレクタの作成（Create a Tag Selector）] ダイアログ ボックスが開きます。「タグ セレクターを作成する （38 ページ）」の手順に従います。

ステップ 6 [**手順 2（STEP 2**） > **セレクタ（Selectors**）] ページで、EPG をエンドポイントセレクタとして指定する場合は、**EPG セレクタ**バーの [+] 記号をクリックします。

[EPG セレクタの作成（Create an EPG Selector）] ダイアログ ボックスが開きます。「EPG セレクタの作成 （39 ページ）」の手順に従います。

ステップ 7 [**手順 2（STEP 2**） > **セレクタ（Selectors**）] ページで、エンドポイントセレクタとして IP サブネットを指定する場合は、**IP サブネットセレクタ**バーの [+] 記号をクリックします。

[**IP サブネット セレクタの作成（Create an IP Subnet Selector**）] ダイアログ ボックスが開きます。「IP サブネット セレクターを作成する （40 ページ）」の手順に従います。

ステップ 8 [次へ（Next）] をクリックします。

[**エンドポイントセキュリティ グループの作成（Create Endpoint Security Group**）] ダイアログボックスの [**手順 3（STEP 3**）] > **[詳細（オプション）（Advanced (Optional)**）] ページが開きます。

ステップ 9 [手順 3（STEP 3）] > [詳細（オプション）（Advanced (Optional)）] ページで、次のオプションを構成できます。

a) （任意） ESG 内の通信をブロックするには、[ESG 内分離（Intra ESG Isolation）] フィールドで [強制（Enforced）] を選択します。デフォルトは [非強制（Unenforced）] です。

[非強制（Unenforced）] では、同じ ESG 内のすべてのエンドポイントが自由に通信できます。または、同じ ESG 内で特定のタイプの通信のみを許可する場合は、代わりに ESG 内コントラクトを使用できます。ESG 内のコントラクト構成については、「GUI を使用して契約をエンドポイント セキュリティ グループに適用する （43 ページ）」 を参照してください。

b) （任意） 設定済みグループメンバーとして ESG を含むには、[設定済みグループメンバー（Preferred Group Member）] フィールドで [含める（Include）] を選択します。デフォルトは [除外（Exclude）] です。

[含める（Include）] を選択する前に、優先グループが VRF レベルで有効になっていることを確認してください。

設定済みグループの詳細については、『*Cisco APIC* 基本構成ガイド』を参照してください。

c) （任意） 別の ESG からコントラクトを継承するには、**ESG コントラクトマスター**バーの [+] 記号をクリックし、コントラクトを継承する ESG を選択します。

ESG コントラクトマスターを選択した場合、作成している ESG は、選択した ESG のすべてのコントラクトを継承します。新しい ESG が既存の ESG と同じセキュリティ構成を持つようにする場合は、ESG コントラクトマスターを追加します。

ステップ 10 [Finish] をクリックします。

セレクタとタグを設定する

タグ セレクターを作成する

この手順を使用して、エンドポイント セキュリティ グループ (ESG) のタグ セレクターを作成します。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[タグ セレクター（Tag Selectors）]** を右クリックし、**[タグ セレクターの作成（Create a Tag Selector）]** を選択します。

ステップ 4 **[タグ セレクターの作成（Create an Tag Selector）]** ダイアログ ボックスに、次の情報を入力します。

a) **タグ キー**：タグ キーを入力するか、ドロップダウン リストから既存のタグ キーを選択します。

b) **値演算子**：ESG に含めるエンティティのタグ値を一致させるための条件を選択します。

選択できる演算子は次の通りです。

- **Contains**：タグ値を含むが、**[タグ値（Tag Value）]** と完全に一致しない可能性があるエンティティを選択します。
- **Equals**：タグ値が **[タグ値（Tag Value）]** と等しいエンティティを選択します。
- **Regex**：タグ値が **[タグ値（Tag Value）]** フィールドに入力された正規表現と一致するエンティティを選択します。

c) **タグ値**：値または正規表現を入力するか、ドロップダウン リストから既存の値を選択します。

正規表現を作成するときは、次のガイドラインを使用してください。

- 有効な文字は、a-z A-Z 0-9 _ . です。, : ^ $ [] () {} | + * -
- 次の文字は使用できません。/ \ ?
- [0-9]+ は任意の数に一致（\d+ と同等）
- a{0,1} は、a のゼロまたは 1 つに一致します（? と同等）
- [0-9]{3} は 3 桁の数字に完全に一致します
- dev(1)|(2) は dev1 または dev2 の値に一致します

d) **説明**：（オプション）オブジェクトの説明。

e) [送信（Submit）] をクリックします。

EPG セレクタの作成

この手順を使用して、エンドポイント セキュリティ グループ (ESG) の EPG セレクタを作成します。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[EPG セレクタ（EPG Selectors）]** を右クリックし、**[EPG セレクタの作成（Create an EPG Selector）]** を選択します。

ステップ 4 **[EPG セレクタの作成（Create an EPG Selector）]** ダイアログ ボックスに、次の情報を入力します。

a) **ESG VRF の EPG**：VRF に存在する EPG のリストから、ESG に含まれる EPG のチェックボックスをオンにします。

b) **説明**：（オプション）オブジェクトの説明。

c) [送信（Submit）] をクリックします。

IP サブネット セレクターを作成する

この手順を使用して、エンドポイント セキュリティ グループ（ESG）の IP サブネット セレクターを作成します。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[IP サブネット セレクター（IP Subnet Selectors）]** を右クリックし、**[IP サブネット セレクターの作成（Create an IP Subnet Selector）]** を選択します。

ステップ 4 **[IP サブネット セレクターの作成（Create an IP Subnet Selector）]** ダイアログ ボックスで、次の情報を入力します。

a) **IP サブネット**：**キー**：このフィールドは **IP** に設定されています。

b) **IP サブネット**：**演算子**：このフィールドは**等しい**に設定されています。セレクターは、指定されたサブネットに完全に一致する IP サブネットのみに一致します。

c) **IP サブネット**：値 : ESG に含まれるエンドポイントの IP サブネットを入力します。

特定の IP (/32、/128、またはサブネット マスクなし) または任意のマスク長のサブネット マッチを入力できます。

d) **説明**：（オプション）

e) [送信（Submit）] をクリックします。

サービス EPG セレクターを作成する

この手順を使用して、エンドポイント セキュリティ グループ（ESG）のサービス EPG セレクターを作成します。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[サービス EPG セレクター（Service EPG Selectors）]** を右クリックし、**[サービス EPG セレクターの作成（Create a Service EPG Selector）]** を選択します。

ステップ 4 **[サービス EPG セレクターの作成（Create a Service EPG Selector）]** ダイアログ ボックスに、次の情報を入力します。

a) **サービス EPG**：サービス EPG を ESG に含めるには、提供されているサービス デバイス コネクタのリストから選択します。

サービス EPG を表すサービス デバイス コネクタ（LifCtx）は、ESG にマッピングできます。表示されるサービス デバイス コネクタのリストは、次の場所にあるデバイス選択ポリシーで定義されたコネクタから取得されます。

Tenants > ***tenant_name*** > **Services** > **L4-L7** > **Device Selection Policies**

サービス デバイス コネクタは、次の形式で表示されます。

consumer または **provider**

TENANT_NAME/c-*CONTRACT_NAME*-g-*GRAPH_NAME*-n-*NODE_NAME*

次に例を示します。

コンシューマ

PBR/c-web-to-app-g-FW-Graph-n-N1

b) **説明**：（オプション）オブジェクトの説明。
c) [送信（Submit）] をクリックします。

エンドポイント MAC タグを作成する

この手順を使用して、ポリシー タグをエンドポイントの MAC アドレスに追加します。タグ セレクタは、このタグを使用して、エンドポイントの MAC アドレスをエンドポイント セキュリティ グループ (ESG) に関連付けることができます。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[アプリケーション EPG（Application EPGs）]** > ***[epg_name]*** を展開します。

ステップ 3 [作業（Work）] ペインで、**[操作（Operational）]** > **[クライアント エンドポイント（Client Endpoints）]** タブを選択します。

[クライアント エンドポイント（Client Endpoints）] には、関連付けられている IP アドレスとともに、利用可能な各エンドポイントの MAC アドレスを表示します。アドレスにすでにポリシー タグが割り当てられている場合、それらのポリシー タグは MAC または IP アドレスの **[ポリシー タグ（Policy Tags）]** 列に表示されます。

ステップ 4 目的の MAC アドレスの行を右クリックし、**[エンドポイント MAC タグの設定（Configure an Endpoint MAC Tag）]** を選択します。

MAC アドレスがテーブルに表示されない場合は、VMM 統合を通じてまだ学習または表示されていません。この場合、***[tenant_name]*** > **[ポリシー（Policies）]** > **[エンドポイント タグ（Endpoint Tags）]** を展開し、**[エンドポイント MAC（Endpoint MAC）]** を右クリックし、**[エンドポイント MAC タグの作成（Create an Endpoint MAC Tag）]** を選択します。

ステップ 5 **[エンドポイント MAC タグの作成（Create an Endpoint MAC Tag）]** ダイアログ ボックスに次の情報を入力します。

（注） **[クライアント エンドポイント（Client Endpoints）]** テーブルから MAC アドレスを選択した場合、MAC アドレスと BD フィールドはすでに入力されています。

a) **エンドポイント MAC アドレス**：タグを追加する MAC アドレスを入力します。

b) **BD 名**：既存のブリッジ ドメインを選択するか、新しいブリッジ ドメインを作成します。

***** を選択すると、エンドポイント MAC タグは、指定された VRF 内の任意の BD の MAC アドレスを表します。この場合、VRF も選択するよう求められます。

c) **注釈**：（オプション）**[+]** 記号をクリックし、注釈キーと値を追加し、[✓] 記号をクリックします。

複数の注釈を追加できます。

d) **ポリシー タグ**：**[+]** 記号をクリックし、ポリシー タグ キーと値を追加し、[✓] 記号をクリックします。

複数のポリシー タグを追加できます。

e) [送信（Submit）] をクリックします。

エンドポイント IP タグの作成

この手順を使用して、エンドポイント IP アドレスにポリシー タグを追加します。タグ セレクターは、このタグを使用して、エンドポイントの IP アドレスをエンドポイント セキュリティ グループ (ESG) に関連付けることができます。

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[アプリケーション EPG（Application EPGs）]** > ***[epg_name]*** を展開します。

ステップ 3 [作業（Work）] ペインで、**[操作（Operational）]** > **[クライアント エンドポイント（Client Endpoints）]** タブを選択します。

[クライアント エンドポイント（Client Endpoints）] には、関連付けられている IP アドレスとともに、利用可能な各エンドポイントの MAC アドレスを表示します。アドレスにすでにポリシー タグが割り当てられている場合、それらのポリシー タグは MAC または IP アドレスの **[ポリシー タグ（Policy Tags）]** 列に表示されます。

ステップ 4 目的の IP アドレスの行を右クリックし、**[エンドポイント IP タグの設定（Configure an Endpoint IP Tag）]** を選択します。

IP アドレスがテーブルに表示されない場合、VMM 統合を通じてまだ学習または表示されていません。この場合、***[tenant_name]*** > **[ポリシー（Policies）]** > **[エンドポイント タグ（Endpoint Tags）]** を展開し、**[エンドポイント IP（Endpoint IP）]** を右クリックし、**[エンドポイント IP タグの作成（Create an Endpoint IP Tag）]** を選択します。

ステップ 5 **[エンドポイント IP タグの作成（Create an Endpoint IP Tag）]** ダイアログ ボックスに次の情報を入力します。

[クライアント エンドポイント（Client Endpoints）] テーブルからエンドポイントを選択した場合、IP アドレスと VRF フィールドはすでに入力されています。

a) **IP**：タグを追加する IP アドレスを入力します。
b) **注釈**：（オプション）**[+]** 記号をクリックし、注釈キーと値を追加し、[✓] 記号をクリックします。

複数の注釈を追加できます。

c) **VRF 名**：エンドポイントを含む VRF を選択または作成します。
d) **ポリシー タグ**：**[+]** 記号をクリックし、ポリシー タグ キーと値を追加し、[✓] 記号をクリックします。

複数のポリシー タグを追加できます。

e) [送信（Submit）] をクリックします。

GUI を使用して契約をエンドポイント セキュリティ グループに適用する

ステップ 1 メニュー バーで **[テナント（Tenants）]** を選択し、該当するテナントを選択します。

ステップ 2 左のナビゲーション ペインで、***[tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > ***[application_profile_name]*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > ***[esg_name]*** を選択します。

ステップ 3 **[契約（Contracts）]** を右クリックし、契約が展開される方法に応じてアクションを選択します。

次のオプションがあります。

- **提供されたコントラクトの追加**
- **消費される契約の追加**
- **消費されるコントラクト インターフェイスの追加**
- **ESG 内契約の追加**

（注） アプリケーション EPG によって消費または提供される契約は、ここでは ESG には使用できません。

ステップ 4 [Add Contract] ダイアログボックスで、次の操作を実行します。

a) **[契約名（Contract Name）]** を入力または選択します。
b) （任意） **[QOS ポリシー（QOS policy）]** を選択します。
c) （任意） **[ラベル（Label）]** を選択します。

ステップ 5 [送信（Submit）] をクリックします。

REST API を使用したエンドポイント セキュリティ グループの作成と契約の適用

手順：

```
<polUni>
  <fvTenant name="t0">
    <fvAp name="ap0">
      <!-- ESG with the name ESG1 and Preferred Group as Exclude -->
      <fvESg name="ESG1" prefGrMemb="exclude">
          <!-- The ESG is associated to VRFA -->
          <fvRsScope tnFvCtxName="VRFA" />

          <!-- provided and consumed contracts -->
          <fvRsProv tnVzBrCPName="provided_contract1" />
          <fvRsCons tnVzBrCPName="consumed_contract2" />

          <!-- Tag Selectors for the ESG -->
         <fvTagSelector matchKey="stage" valueOperator="equals" matchValue="production"/>

          <fvTagSelector matchKey="owner" valueOperator="contains" matchValue="teamA"/>
          <fvTagSelector matchKey="__vmm::vmname" valueOperator="regex"
matchValue="web_[0-9]+"/>

          <!-- EPG Selectors for the ESG -->
          <fvEPgSelector matchEpgDn="uni/tn-TK/ap-AP1/epg-EPG1-1"/>
          <fvEPgSelector matchEpgDn="uni/tn-TK/ap-AP1/epg-EPG1-2"/>

          <!-- IP Subnet Selectors for the ESG -->
          <fvEPSelector matchExpression="ip=='192.168.0.1/32'" />
          <fvEPSelector matchExpression="ip=='192.168.1.0/28'" />
          <fvEPSelector matchExpression="ip=='2001:23:45::0:0/64'" />
      </fvESg>
    </fvAp>
  </fvTenant>
</polUni>
```

REST API を使用してタグおよびセレクターを作成する

EPG セレクターを作成する

EPG セレクター オブジェクト（**fvEPgSelector**）は、特定の EPG の DN と一致します。

```
<polUni>
  <fvTenant name="ExampleCorp">
    <fvAp name="AP">
      <fvESg name="esg1">
        <fvEPgSelector matchEpgDn="uni/tn-ExampleCorp/ap-app/epg-epg1"/>
        <fvRsScope tnFvCtxName="dev"/>
      </fvESg>
    </fvAP>
  </fvTenant>
</polUni>
```

EPG セレクターは、ESG と同じテナントおよび VRF に属する EPG にのみ一致できます。

タグとタグ セレクターの作成

タグセレクタオブジェクト（**fvTagSelector**）は、次のオブジェクトの下で検出されたタグオブジェクト（**tagTag**）と一致します。

- **fvEpIpTag**
- **fvEpMacTag**
- **fvSubnet**
- **fvStCEp**

（注） タグ セレクター オブジェクトは、**fvEpVmmMacTagDef** 下のタグ オブジェクトにも一致します。ただし、このオブジェクトの下のポリシータグはVMM統合を通じて設定され、構成できません。

この例は、**tagTag** オブジェクトの位置と、タグを見つけて、一致する **fvTagSelector** オブジェクトを示しています。

```
<polUni>
  <fvTenant name="ExampleCorp">
    <fvEpTags>
      <fvEpIpTag ip="192.168.1.1" ctxName="example">
        <tagTag key="esg" value="Red"/>
       </fvEpIpTag>
    </fvEpTags>


    <fvAp name="AP">
      <fvESg name="esg1">
        <fvRsScope tnFvCtxName="example"/>
        <fvTagSelector matchKey="esg" matchValue="Red"/>
      </fvESg>
    </fvAp>
  </fvTenant>
</polUni>
```

タグを完全に一致させる代わりに、タグを部分的に一致させるか、または **valueOperator** の **fvTagSelector** プロパティを使用して正規表現を使用して一致させることができます。

- **valueOperator** プロパティがない場合、または「等しい」場合は、値が完全に一致する **tagTag** のみが認識されます。
- **valueOperator** プロパティが「含む」の場合、**tagTag** の値フィールドに **fvTagSelector** の **matchValue** フィールドが含まれていても、完全に一致していない場合に一致が認識されます。
- **valueOperator** プロパティが「regex」の場合、**tagTag** の値が **fvTagSelector** の **matchValue** フィールドに含まれる正規表現を満たす場合に一致が認識されます。

この例は、さまざまな一致条件を示しています。

```
<fvTagSelector matchKey="name" matchValue="Blue"/>
<fvTagSelector matchKey="name" matchValue="Blue" valueOperator = "equals"/>
<fvTagSelector matchKey="name" matchValue="prod" valueOperator = "contains"/>
<fvTagSelector matchKey="name" matchValue="prod[0-4]" valueOperator = "regex"/>
```

VMM エンドポイント用の特別なタグ セレクター

特別なキーを使用して、タグ セレクター オブジェクト（**fvTagSelector**）は VMM エンドポイントを名前で照合します。特殊な **matchKey** は「__vmm::vmname」で、**matchValue** は VM の名前です。

この例は、完全一致を使用して「vmName-Dev」という名前の VM に一致するタグ セレクターを示しています。

```
<polUni>
  <fvTenant name="ExampleCorp">
    <fvAp name="AP">
      <fvESg name="esg1">
        <fvTagSelector matchKey="type" matchValue="dev"/>
        <fvTagSelector matchKey="__vmm::vmname" matchValue="vmName-Dev"/>
        <fvRsScope tnFvCtxName="testctx0"/>
      </fvESg>
    </fvAp>
  </fvTenant>
</polUni>
```

エンドポイントセキュリティグループを使用してルートリークを設定する

GUIを使用した内部ブリッジドメインサブネットのルートリークの設定

この手順を使用して、内部ブリッジ ドメイン サブネットのルート リークを設定します。

始める前に

リークするテナント、VRF、ブリッジドメイン、サブネットを作成しておく必要があります。

ステップ 1 [Navigation] ペインで、[Tenant name] > [Networking] > [VRFs] > [Inter-VRF Leaked Routes for ESG] > [EPG/BD Subnets] に移動します。

ステップ 2 **[EPG/BD サブネット（EPG/BD Subnets）]** を右クリックし、**[EPG/BD サブネットをリークするようにに設定する（Configure EPG/BD Subnet to leak）]** を選択します。

ステップ 3 **[EPG/BD サブネットをリークするようにに設定する（Configure EPG/BD Subnet to leak）]** ダイアログ ボックスで、次の機能を実行します。

a) **IP**：リークするブリッジ ドメイン サブネットとそのマスクを入力します。
b) （任意） **説明**：EPG またはブリッジ ドメイン サブネットの説明を入力します。
c) （任意） **L3Out アドバタイズを許可する**：このサブネットを別の VRF の L3Out によってアドバタイズする必要がある場合は、**True** に設定します。

ステップ 4 **[テナントおよび VRF 宛先（Tenant and VRF destinations）]** フィールドで、右に移動し、**[+]** 記号をクリックします。

ステップ 5 **[テナントおよび VRF 宛先の作成（Create Tenant and VRF destination）]** ダイアログ ボックスで、次の機能を実行します。

a) **テナントおよび VRF**：テナントおよび VRF 名を入力または選択します。
b) （任意） **説明**：宛先の説明を入力します。
c) **L3Out アドバタイズメントを許可する**：ターゲット VRF ごとに許可を変更する必要がある場合は、**True** または **False** に設定します。デフォルトでは、このオプションは**継承**するように設定されており、ステップ 3 の **[L3Out アドバタイズを許可する（Allow L3Out Advertisement）]** と同じ設定を保持します。
d) [OK] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

REST API を使用した内部ブリッジ ドメイン サブネットのルート リークの設定

はじめる前に

漏洩する BD サブネット、または漏洩したサブネットを含む BD サブネットを設定しておく必要があります。

手順：

```
<polUni>
  <fvTenant name="t0">
    <fvCtx name="VRFA">
      <leakRoutes>
        <!--
            leak the BD subnet 192.168.1.0/24 with the Allow L3Out Advertisement
            False (i.e. scope private)
        -->
        <leakInternalSubnet ip="192.168.1.0/24" scope="private">
          <!--
              leak the BD subnet to Tenant t1 VRF VRFB with the
              Allow L3Out Advertisement configured in the parent
              scope (i.e. scope inherit)
          -->
          <leakTo ctxName="VRFB" tenantName="t1" scope="inherit" />
        </leakInternalSubnet>
      </leakRoutes>
    </fvCtx>
  </fvTenant>
</polUni>
```

GUI を使用して外部プレフィックスのルートリークを構成する

この手順を使用して、外部プレフィックスのルートリークを構成します。

始める前に

送信元 VRF で L3Out を構成しておく必要があり、外部プレフィックスが学習されます。

ステップ 1 ナビゲーションウィンドウで、[**テナント名（Tenant name**）]>[**ネットワーキング（Networking**）]>[**VRFs**] > [**ESG の VRF 間 リークルート（Inter- VRF Leaked Routes for ESG**）] > [**外部 プレフィックス（External Prefixes**）] の順に選択します。

ステップ 2 [**外部プレフィックス（External Prefixes**）] を右クリックし、[**リークされた外部プレフィックスの作成（Create Leaked External Prefix**）]を選択します。

ステップ 3 [**リークされた外部プレフィックスの作成（Create Leaked External Prefix**）] ダイアログボックスで、次の操作を実行します。

a) **IP**：リークされたプレフィックスを入力します。

b) （任意） **説明**：リークされた外部プレフィックスの説明を入力します。

c) （任意） **以上（プレフィックス）**：照合するプレフィックスの最小長を入力します。これは、通常のルータの IP プレフィックスリストの「ge」に相当します。

d) （任意） **以下（プレフィックス）**：照合するプレフィックスの最大長を入力します。これは、通常のルータの IP プレフィックスリストの「le」に相当します。

ステップ 4 **[テナントおよび VRF 宛先（Tenant and VRF destinations）]** フィールドで、右に移動し、**[+]** 記号をクリックします。

ステップ 5 **[テナントおよび VRF 宛先の作成（Create Tenant and VRF destination）]** ダイアログ ボックスで、次の機能を実行します。

a) **テナントおよび VRF**：テナントおよび VRF 名を入力または選択します。

b) （任意） **説明**：宛先の説明を入力します。

c) [OK] をクリックします。

ステップ 6 [送信（Submit）] をクリックします。

REST API を使用して外部プレフィックスのルート リークを設定する

はじめる前に

ソース VRF「VRFA」で L3Out を設定しておく必要があり、外部プレフィックスが学習されます。

手順：

```
<polUni>
  <fvTenant name="t0">
    <fvCtx name="VRFA">
      <leakRoutes>
        <!--
```

```
            leak the external prefixes in the range of
            10.20.0.0/17 and 10.20.0.0/30
          -->
          <leakExternalPrefix ip="10.20.0.0/16" ge="17" le="30">
            <!-- leak the external prefixes to Tenant t1 VRF VRFB -->
            <leakTo ctxName="VRFB" tenantName="t1" />
          </leakExternalPrefix>
        </leakRoutes>
      </fvCtx>
    </fvTenant>
</polUni>
```

エンドポイントセキュリティ グループを使用したレイヤ 4 からレイヤ 7 を設定する

GUI を使用してエンドポイントセキュリティ グループへのレイヤ 4 ～ レイヤ 7 サービスを適用する

EPG を使用したサービス グラフの展開に提供されるすべての構成は、同様に ESG にも適用されます。必要な変更は、EPG にコントラクトを関連付ける代わりに ESG にコントラクトを関連付けることのみです。この手順を使用して、エンドポイントセキュリティ グループによって使用されるコントラクトに、非管理モードのレイヤ 4 ～ レイヤ 7 サービスデバイスのサービス グラフテンプレートを適用します。

始める前に

次を作成しておく必要があります。

- ESG
- サービス グラフ テンプレート

ステップ 1 メニュー バーで、**[テナント（Tenants）] > [すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーションウィンドウで、**[テナント（Tenant）] > [サービス（Services）] > [L4-L7] > [サービスグラフテンプレート（Service Graph Templates）]** の順に選択します。

ステップ 4 ナビゲーションウィンドウで、ESG に適用する **[サービスグラフテンプレート名（Service Graph Template Name）]** を右クリックし、**[L4 ～ L7 サービスグラフテンプレートを適用する（Apply L4-L7 Service Graph Template）]** を選択します。

Apply L4-L7 Service Graph Template To EPGs ダイアログボックスが表示されます。レイヤ 4 ～ レイヤ 7 サービスグラフテンプレートを、エンドポイントセキュリティ グループ間のコントラクトに関連付けます。

ステップ 5 適切な値を入力して、**[L4 ～ L7 サービスグラフテンプレートを ESG に適用する（Apply L4-L7 Service Graph Template To EPGs）手順 1（STEP 1）] > [コントラクト（Contract）]** ダイアログボックスのコントラクトを構成します。

a) エンドポイント グループタイプとして **[エンドポイントセキュリティ グループ（Endpoint Security Group）]** を選択します。

b) ESG 内コントラクトを構成している場合は、**[エンドポイント内コントラクトを構成する（Configure an Intra-Endpoint Contract）]** チェックボックスをオンにして、**[ESG/ネットワーク（ESG / Network）]** ドロップダウンリストから ESG を選択します。

c) ESG 内コントラクトではなく通常のコントラクトを使用している場合は、コンシューマーとプロバイダーの ESG とネットワークの組み合わせを選択します。

d) **[コントラクトタイプ（Contract Type）]** フィールドで適切なオプションボタンをクリックして、新しいコントラクトを作成するか既存のコントラクトを選択します。[Create A New Contract] を選択した場合、フィルタを設定するには、[No Filter (Allow All Traffic)] チェックボックスをオフにします。[+] をクリックしてフィルタ エントリを追加し、完了したら [Update] をクリックします。

ステップ 6 [次へ] をクリックします。

[STEP 2] > [Graph] ダイアログが表示されます。

ステップ 7 **[ご使用のデバイス情報（your device name Information）]** セクションで、赤いボックスで示されている必須フィールドでを構成します。

ステップ 8 **[Finish（完了）]** をクリックします。

これで、ESG が使用するコントラクトにサービスグラフテンプレートを適用できました。

（注） vzAny を構成するには、上記の手順 5.c で、プロバイダーとして **AnyEPG** を選択し、コンシューマーとして関心のある ESG を選択するか、またはその逆を選択します。

サービス グラフを vzAny-to-vzAny コントラクト vzAny-vzAny に適用するには、エンドポイントグループタイプとして **[エンドポイントポリシーグループ（EPG）（Endpoint Policy Group (EPG)）]** を選択し、プロバイダーおよびコンシューマーとして **[AnyEPG]** を選択します。

REST API を使用したエンドポイント セキュリティ グループへのレイヤ 4 からレイヤ 7 サービスの適用

EPG を使用してサービス グラフを展開するために提供されるすべての REST API は、ESG にも等しく適用されます。ただし、契約は ESG に関連付けられている必要があります。

詳細については、レイヤ 4 からレイヤ 7 の REST API の例を参照してください。

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。