ACI ファブリックの基本

この章の内容は、次のとおりです。

- ACI ファブリックの基本について，1 ページ
- ID と場所の分離，2 ページ
- ポリシー ID と適用，2 ページ
- カプセル化の正規化，4 ページ
- マルチキャスト ツリー トポロジ，4 ページ
- ロード バランシング，6 ページ
- エンドポイントの保持，7 ページ
- ACI ファブリック セキュリティ ポリシー モデル，8 ページ

ACI ファブリックの基本について

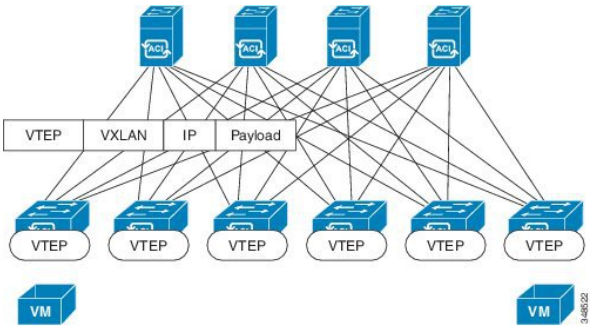
ACI ファブリックは、64,000 以上の専用テナント ネットワークをサポートしています。 単一のファブリックは、100 万以上の IPv4/IPv6 エンドポイント、64,000 以上のテナント、および 200,000 以上の 10G ポートをサポートできます。 ACI ファブリックにより、物理サービスと仮想サービス間を接続する追加のソフトウェアやハードウェア ゲートウェイを必要とすることなくサービス（物理または仮想）がどこでも可能になり、Virtual Extensible Local Area Network（VXLAN）/VLAN/Network Virtualization using Generic Routing Encapsulation（NVGRE）のカプセル化が正規化されます。

ACI ファブリックは、基盤となる転送グラフからエンドポイント アイデンティティおよび関連するポリシーを分離します。 また、最適なレイヤ 3 およびレイヤ 2 フォワーディングを保証する分散レイヤ 3 ゲートウェイが提供されます。 ファブリックは、一般的な場所の制約（あらゆる場所の IP アドレス）なしで標準のブリッジングおよびルーティングのセマンティックをサポートし、IP コントロール プレーンの Address Resolution Protocol（ARP）/Generic Attribute Registration Protocol（GARP）に関するフラッディング要件を削除します。 ファブリック内のすべてのトラフィックは、VXLAN 内にカプセル化されます。

ID と場所の分離

ACI ファブリックは、テナント エンドポイント アドレスとその識別子をそのロケータまたは VXLAN トンネルエンドポイント（VTEP）のアドレスで定義されるエンドポイントの場所から切り離します。 次の図は、分離された ID および場所を示します。

図 *1*：*ID* と場所の分離



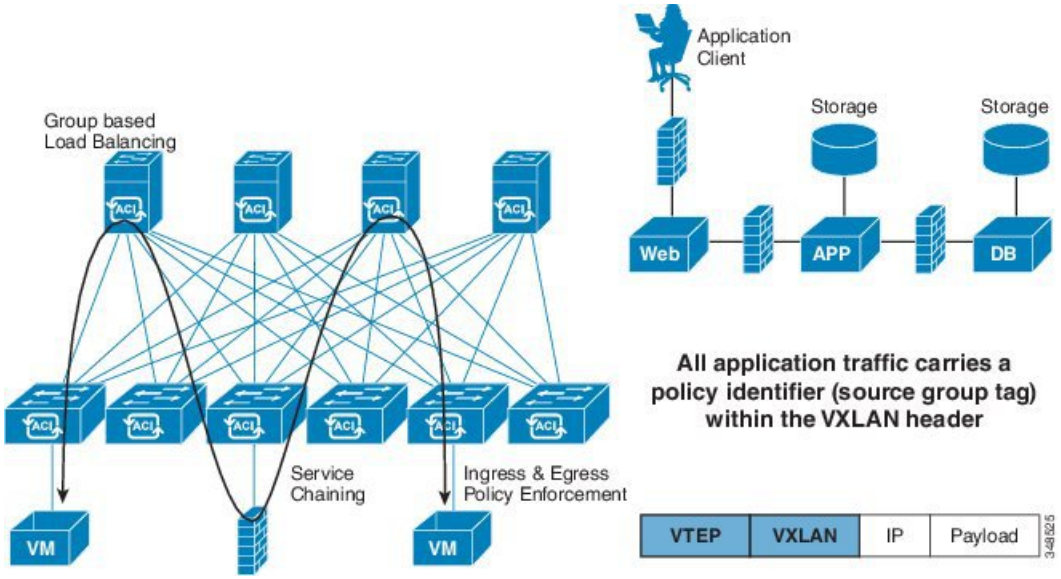
ファブリック内の転送は VTEP 間で行われます。 ある場所への内部テナント MAC または IP アドレスのマッピングは、分散マッピング データベースを使用して VTEP によって実行されます。

ポリシー ID と適用

アプリケーション ポリシーは、VXLAN パケットでも送信される個別のタギング属性を使用して転送から分離されます。 ポリシー ID は、ACI ファブリック内のすべてのパケットで送信され、

完全に分散した形でポリシーの一貫した適用を行うことができます。 次の図は、ポリシー ID を示します。

図 *2*：ポリシー *ID* と適用

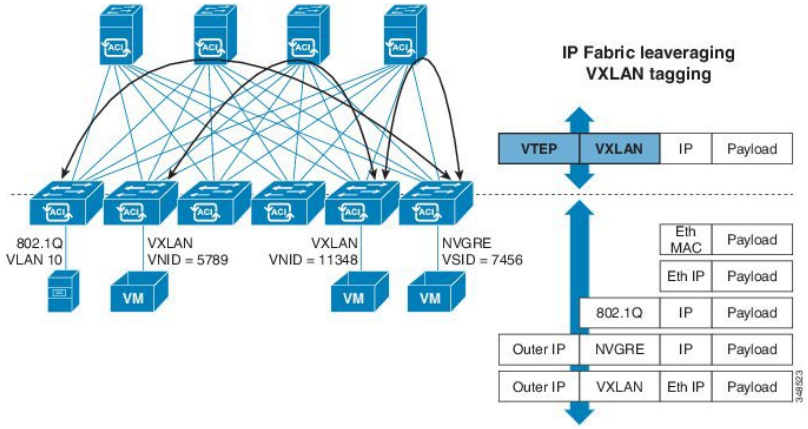


ファブリックおよびアクセスポリシーは、内部のファブリックインターフェイスおよび外部のアクセスインターフェイスの動作を管理します。 システムは、デフォルトのファブリックおよびアクセスポリシーを自動的に作成します。 ファブリックの管理者（ファブリック全体へのアクセス権がある者）は、要件に応じてデフォルトのポリシーを変更したり、新しいポリシーを作成できます。 ファブリックおよびアクセスポリシーにより、さまざまな機能やプロトコルを有効にできます。 APIC のセレクタにより、ファブリックの管理者は、ポリシーを適用するノードおよびインターフェイスを選択できます。

カプセル化の正規化

ファブリック内のトラフィックは、VXLAN としてカプセル化されます。 外部の VLAN/VXLAN/NVGRE タグは、内部の VXLAN タグへのイングレスでマッピングされます。 次の図は、カプセル化の正規化を示します。

図 *3*：カプセル化の正規化



転送は、カプセル化のタイプまたはカプセル化のオーバーレイ ネットワークによって制限または制約されません。外部識別子は、リーフまたはリーフポートにローカライズされ、必要に応じて再利用または変換できます。 ブリッジ ドメインのフォワーディング ポリシーは、必要な場合に標準の VLAN 動作を提供するために定義できます。

マルチキャスト ツリー トポロジ

ACI ファブリックは、アクセス ポートからのユニキャスト、マルチキャスト、およびブロードキャスト トラフィックの転送をサポートします。 エンドポイント ホストからのすべてのマルチデスティネーション トラフィックは、ファブリックにマルチキャスト トラフィックとして伝送されます。

ACI ファブリックは、入力インターフェイスに入るトラフィックを使用可能な中間ステージのスパイン スイッチを介して関連する出力スイッチにルーテッドできる Clos トポロジ（Charles Clos にちなんで名付けられた）に接続されるスパインおよびリーフ スイッチで構成されます。 リーフ スイッチには次の 2 種類のポートがあります。スパイン スイッチに接続するためのファブリック ポートと、サーバ、サービス アプライアンス、ルータ、ファブリック エクステンダ（FEX）などを接続するアクセス ポートです。

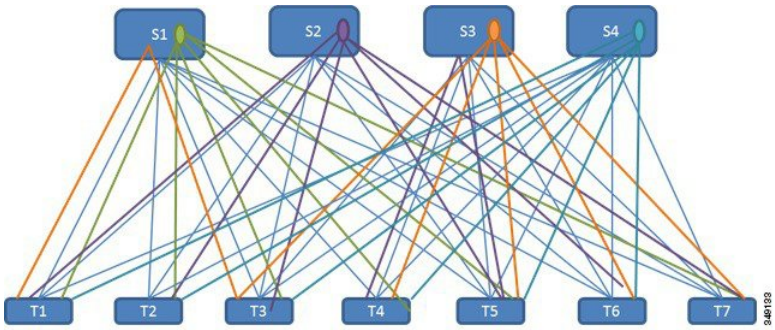
トップ オブ ラック（ToR）スイッチはリーフ スイッチで、スパイン スイッチに接続されます。リーフ スイッチは互いに接続されず、スパイン スイッチはリーフ スイッチのみに接続します。この Clos トポロジでは、すべての下位層のスイッチがフルメッシュ トポロジの最上位層のスイッチにそれぞれ接続されます。 スパイン スイッチが故障すると、ACI ファブリック全体のパフォー

マンスだけがわずかに低下します。 データ パスは、トラフィック負荷がスパイン スイッチ間で均等に分散されるように選択されます。

ACI ファブリックは、Forwarding Tag（FTAG）ツリーを使用してバランス マルチデスティネーション トラフィックをロードします。 すべてのマルチデスティネーション トラフィックは、ファブリック内でカプセル化された IP マルチキャスト トラフィックの形式で転送されます。 入力リーフは、FTAG をスパインに転送するときにトラフィックに割り当てます。 FTAG は宛先マルチキャスト アドレスの一部としてパケットに割り当てられます。 ファブリックでは、トラフィックは指定された FTAG ツリーに沿って転送されます。 スパインおよび中間リーフ スイッチは、FTAG ID に基づいてトラフィックを転送します。 転送ツリーは、FTAG ID 1 つにつき 1 個構築されます。 任意の 2 つのノード間で、FTAG 1 つにつきリンク 1 つだけが転送されます。 複数の FTAG を使用することで、転送に異なるリンクを使用している各 FTAG でパラレル リンクを使用できます。 ファブリック内の FTAG ツリーの数が多いほど、ロード バランシングの効果が大きい可能性があるということになります。 ACI ファブリックは、最大 12 個の FTAG をサポートします。

次の図は、4 つの FTAG によるトポロジを示します。 ファブリック内のすべてのリーフ スイッチは、各 FTAG に直接または中継ノードを介して接続されます。 1 つの FTAG が各スパイン ノードに根付いています。

図 *4*：マルチキャスト ツリー トポロジ



リーフ スイッチはスパインへの直接接続性がある場合、直接パスを使用して FTAG ツリーに接続します。 直接リンクがない場合、リーフ スイッチは上記の図に示すように FTAG ツリーに接続されている中継ノードを使用します。 図には、各スパインが 1 つの FTAG ツリーのルートとして示されていますが、複数の FTAG ツリー ルートを 1 つのノード上に置くことができます。

ACI ファブリック起動検出プロセスの一環として、FTAG ルートはスパイン スイッチに配置されます。 APIC は、各スパイン スイッチをスパインがアンカーする FTAG で設定します。 ルートの ID と FTAG の数は設定から取得されます。 APIC は、使用される FTAG ツリーの数と各ツリーに対するルートを指定します。 FTAG ツリーは、ファブリックでトポロジの変更があるたびに再計算されます。

ルートの配置は誘導される設定で、スパイン スイッチの障害などのランタイム イベントで動的に再度ルート付けされることはありません。 通常、FTAG 設定はスタティックです。 スパイン スイッチの追加または削除時は、管理者がスパイン スイッチの残りのセットまたは拡張セット間で FTAG を再配布することを決める可能性があるため、FTAG はあるスパインから別のスパインへ再アンカーできます。

ロード バランシング

ACI ファブリックでは、利用可能なアップリンク リンク間のトラフィックを平衡化するためのロード バランシング オプションがいくつか提供されます。 スタティック ハッシュ ロード バランシングは、各フローが 5 タプルのハッシュに基づいてアップリンクに割り当てられるネットワークで使用される従来のロード バランシング機構です。 このロード バランシングにより、使用可能なリンクにほぼ均等な流量が分配されます。 通常、流量が多いと、流量の均等な分配により帯域幅も均等に分配されます。 ただし、いくつかのフローが残りよりも多いと、スタティック ロード バランシングにより完全に最適ではない結果がもたらされる場合があります。

ダイナミック ロードバランシング（DLB）により、輻輳レベルに従ってトラフィックの割り当てが調整されます。 DLB では、使用可能なパス間の輻輳が測定され、輻輳状態が最も少ないパスにフローが配置されるので、データが最適またはほぼ最適に配置されます。

DLB は、フローまたはフローレットの粒度を使用して使用可能なアップリンクにトラフィックを配置するように設定できます。 フローレットは、時間の大きなギャップによって適切に区切られるフローからのパケットのバーストです。 パケットの 2 つのバースト間のアイドル間隔が使用可能なパス間の遅延の最大差より大きい場合、2 番目のバースト（またはフローレット）を 1 つ目とは異なるパスに沿ってパケットのリオーダーなしで送信できます。 このアイドル間隔は、フローレット タイマーと呼ばれるタイマーによって測定されます。 フローレットにより、パケット リオーダーを引き起こすことなくロード バランシングに対する粒度の高いフローの代替が提供されます。

DLB 動作モードは積極的または保守的です。 これらのモードは、フローレット タイマーに使用するタイムアウト値に関係します。 アグレッシブ モードのフローレット タイムアウトは比較的小さい値です。 この非常に精密なロード バランシングはトラフィックの分配に最適ですが、パケット リオーダーが発生する場合があります。ただし、アプリケーションのパフォーマンスに対する包括的なメリットは、保守的なモードと同等かそれよりも優れています。 保守的なモードのフローレット タイムアウトは、パケットが並び替えられないことを保証する大きな値です。 新しいフローレットの機会の頻度が少ないので、トレードオフは精度が低いロード バランシングです。 DLB は常に最も最適なロードバランシングを提供できるわけではありませんが、スタティック ハッシュ ロード バランシングより劣るということはありません。

ACI ファブリックは、リンクがオフラインまたはオンラインになったことで使用可能なリンク数が変化すると、トラフィックを調整します。 ファブリックは、リンクの新しいセットでトラフィックを再分配します。

スタティックまたはダイナミックのロード バランシングのすべてのモードでは、トラフィックは、Equal Cost Multipath（ECMP）の基準を満たすアップリンクまたはパス上でのみ送信され、これらのパスはルーティングの観点から同等で最もコストがかかりません。

ロード バランシング技術ではありませんが、Dynamic Packet Prioritization（DPP）は、スイッチで DLB と同じメカニズムをいくつか使用します。 DPP の設定は DLB 専用です。 DPP は、長いフローよりも短いフローを優先します。短いフローは約 15 パケット未満です。 短いフローは、長いフローより遅延に敏感です。 DPP により、アプリケーション全体のパフォーマンスが向上します。

ACI ファブリックのデフォルト設定では、従来の静的なハッシュが使用されます。 静的なハッシュ機能により、アップリンク間のトラフィックがリーフ スイッチからスパイン スイッチに分配されます。 リンクがダウンまたは起動すると、すべてのリンクのトラフィックが新しいアップリンク数に基づいて再分配されます。

エンドポイントの保持

スイッチでキャッシュ エンドポイントのMACアドレスとIPアドレスを保持することで、パフォーマンスが向上します。 スイッチは、アクティブになるときにエンドポイントについて学習します。 ローカル エンドポイントはローカル スイッチにあります。 リモート エンドポイントは他のスイッチにありますが、ローカルでキャッシュされます。リーフ スイッチは、直接（または直接接続されたレイヤ 2 スイッチまたはファブリック エクステンダを通じて）接続されたエンドポイント、ローカルエンドポイント、およびファブリックの他のリーフ スイッチに接続されたエンドポイント（ハードウェアのリモート エンドポイント）に関する場所とポリシーの情報を保存します。 スイッチは、ローカル エンドポイントには 32 Kb エントリ キャッシュを、リモート エンドポイントには 64 Kb エントリ キャッシュを使用します。

リーフ スイッチで稼働するソフトウェアは、これらのテーブルを能動的に管理します。 ローカル的に接続されたエンドポイントでは、ソフトウェアは各エントリの保持タイマーの期限切れ後にエントリをエージング アウトします。 エンドポイント エントリは、エンドポイントのアクティビティが終了するとスイッチ キャッシュからプルーニングされ、エンドポイントの場所が他のスイッチに移動するか、またはライフサイクルの状態がオフラインに変わります。 ローカル保持タイマーのデフォルト値は 15 分です。 非アクティブのエントリを削除する前に、リーフ スイッチはエンドポイントに 3 つの ARP 要求を送信し、実際になくなっているかを確認します。 リモートで接続されたエンドポイントの場合、スイッチは非アクティブになってから 3 分後にエントリをエージング アウトします。 リモート エンドポイントは、再度アクティブになるとテーブルにすぐに再入力されます。 エンドポイントが再度キャッシュされるまでリモート リーフ スイッチで適用されるポリシー以外にテーブルにリモート エンドポイントがなくても、パフォーマンスのペナルティはありません。

エンドポイントの保持タイマー ポリシーは変更できます。 スタティック エンドポイントの MAC およびIPアドレスを設定すると、保持タイマーをゼロに設定することで、スイッチ キャッシュに永久的に保存できます。 エントリの保持タイマーをゼロに設定することは、それが削除されないことを意味します。 この操作は慎重に行う必要があります。 エンドポイントが移動したりポリシーが変化する場合は、APIC を介してエントリを最新情報に更新する必要があります。 保持タイマーがゼロ以外の場合、この情報は APIC の介入なしで各パケットで確認されほぼ瞬時に更新されます。

エンドポイントの保持ポリシーは、プルーニングがどのように行われるかを決定します。 ほとんどの場合、デフォルトのポリシーアルゴリズムが使用されます。エンドポイントの保持ポリシーを変更すると、システムパフォーマンスに影響を与える場合があります。何千ものエンドポイントと通信するスイッチの場合、エージング間隔を短くすると、多数のアクティブなエンドポイントをサポートするのに使用可能なキャッシュ ウィンドウの数が増えます。エンドポイントの数が 10,000 を超える場合は、複数のスイッチにエンドポイントを分散させることを推奨します。

ACI ファブリック セキュリティ ポリシー モデル

ACI のファブリック セキュリティ ポリシー モデルはコントラクトに基づいています。 このアプローチにより、従来のアクセス コントロール リスト（ACL）の制限に対応できます。 コントラクトには、エンドポイントグループ間のトラフィックで適用されるセキュリティポリシーの仕様が含まれます。

EPG 通信にはコントラクトが必要です。EPG/EPG 通信はコントラクトなしでは許可されません。APIC は、コントラクトや関連する EPG などのポリシー モデル全体を各スイッチの具象モデルにレンダリングします。 入力時に、ファブリックに入るパケットはすべて、必要なポリシーの詳細でマークされます。 EPG の間を通過できるトラフィックの種類を選択するためにコントラクトが必要とされるので、コントラクトはセキュリティポリシーを適用します。 コントラクトは、従来のネットワーク設定でのアクセスコントロールリスト（ACL）によって扱われるセキュリティ要件を満たす一方で、柔軟性が高く、管理が容易な、包括的なセキュリティポリシー ソリューションです。

アクセス コントロール リストの制限

従来のアクセス コントロール リスト（ACL）には、ACI ファブリック セキュリティ モデルが対応する多数の制限があります。 従来の ACL は、ネットワーク トポロジと非常に強固に結合されています。 それらは通常、ルータまたはスイッチの入力および出力インターフェイスごとに設定され、そのインターフェイス、およびそれらのインターフェイスを流れることが予期されるトラフィックに合わせてカスタマイズされます。 このカスタマイズにより、それらは多くの場合インターフェイス間で再利用できません。もちろんこれはルータまたはスイッチ間にも当てはまります。

従来の ACL は、非常に複雑で曖昧です。なぜなら、そのリストには、許可された特定の IP アドレス、サブネット、およびプロトコルのリストと、明確に許可されていない多くのものが含まれているためです。 この複雑さは、問題が生じるのを管理者が懸念して ACL ルールを削除するのを躊躇するため、維持が困難で、多くの場合は増大するだけということを意味します。 複雑さは、それらが通常 WAN と企業間または WAN とデータセンター間の境界などのネットワーク内の特定の境界ポイントでのみ配置されていることを意味します。この場合、ACL のセキュリティのメリットは、エンタープライズ内またはデータセンターに含まれるトラフィック向けには生かされません。

別の問題として、1 つの ACL 内のエントリ数の大幅増加が考えられます。 ユーザは多くの場合、一連の送信元が一連のプロトコルを使用して一連の宛先と通信するのを許可する ACL を作成します。 最悪の場合、*N* の送信元が *K* のプロトコルを使用して *M* の宛先と対話する場合、ACL に *N*M*K* の行が存在する場合があります。 ACL は、プロトコルごとに各宛先と通信する各送信元を一覧表示する必要があります。また、ACL が非常に大きくなる前に多くのデバイスやプロトコルを取得することはありません。

ACI ファブリック セキュリティ モデルは、これらの ACL の問題に処理します。 ACI ファブリック セキュリティ モデルは、管理者の意図を直接表します。 管理者は、連絡先、フィルタ、およびラベルの管理対象オブジェクトを使用してエンドポイントのグループがどのように通信するか

を指定します。 これらの管理対象オブジェクトは、ネットワークのトポロジに関連していません。なぜなら、それらは特定のインターフェイスに適用されないためです。 それらは、エンドポイントのこれらのグループの接続場所に関係なく、ネットワークが強要しなければならない簡易なルールです。 このトポロジの独立性は、これらの管理対象オブジェクトが特定の境界ポイントとしてだけではなくデータセンター全体にわたって容易に配置して再利用できることを意味します。

ACI ファブリック セキュリティ モデルは、エンドポイントのグループ化コンストラクトを直接使用するため、サーバのグループが相互に通信できるようにするための概念はシンプルです。 1 つのルールにより、任意の数の送信元が同様に任意の数の宛先と通信することを可能にできます。このようなサイズの縮小により、そのスケールと保守性が大幅に向上します。つまり、データセンター全体でより簡単に使用できることにもつながります。

セキュリティ ポリシー仕様を含むコントラクト

ACI セキュリティ モデルでは、コントラクトに EPG 間の通信を管理するポリシーが含まれます。コントラクトは通信内容を指定し、EPG は通信の送信元と宛先を指定します。 コントラクトは次のように EPG をリンクします。

EPG 1 ---------- コントラクト ---------- EPG 2

コントラクトで許可されていれば、EPG 1 のエンドポイントは EPG 2 のエンドポイントと通信でき、またその逆も可能です。 このポリシーの構造には非常に柔軟性があります。 たとえば、EPG 1 と EPG2 間には多くのコントラクトが存在でき、1 つのコントラクトを使用する EPG が 3 つ以上存在でき、コントラクトは複数の EPG のセットで再利用できます。

また EPG とコントラクトの関係には方向性があります。 EPG はコントラクトを提供または消費できます。 コントラクトを提供する EPG は通常、一連のクライアント デバイスにサービスを提供する一連のエンドポイントです。 そのサービスによって使用されるプロトコルはコントラクトで定義されます。 コントラクトを消費する EPG は通常、そのサービスのクライアントである一連のエンドポイントです。 クライアント エンドポイント（コンシューマ）がサーバ エンドポイント（プロバイダー）に接続しようとすると、コントラクトはその接続が許可されるかどうかを確認します。 特に指定のない限り、そのコントラクトは、サーバがクライアントへの接続を開始することを許可しません。 ただし、EPG 間の別のコントラクトが、その方向の接続を簡単に許可する場合があります。

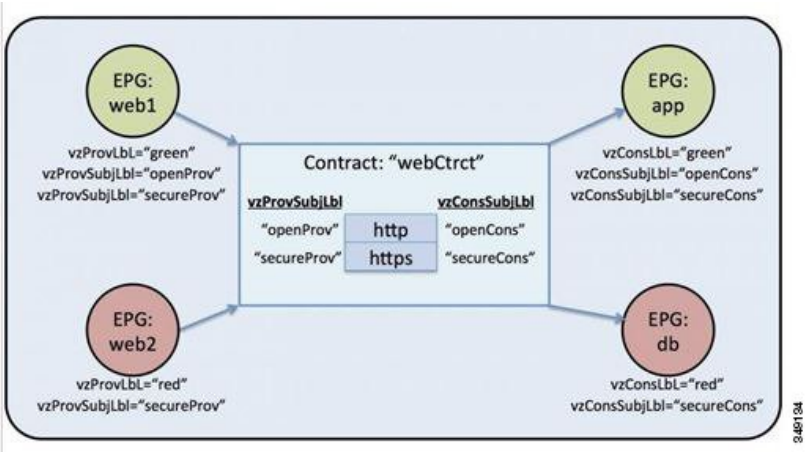
この提供/消費の関係は通常、EPG とコントラクト間を矢印を使って図で表されます。 次に示す矢印の方向に注目してください。

EPG 1 <------- 消費 -------- コントラクト <------- 提供 -------- EPG 2

コントラクトは階層的に構築されます。 1 つ以上のサブジェクトで構成され、各サブジェクトには 1 つ以上のフィルタが含まれ、各フィルタは 1 つ以上のプロトコルを定義できます。

次の図は、コントラクトが EPG の通信をどのように管理するかを示します。

図 *5*： *EPG/EPG* 通信を決定するコントラクト



たとえば、TCP ポート 80 とポート 8080 を指定する HTTP と呼ばれるフィルタと、TCP ポート 443 を指定する HTTPS と呼ばれる別のフィルタを定義できます。 その後、2 セットのサブジェクトを持つ webCtrct と呼ばれるコントラクトを作成できます。 openProv および openCons は HTTP フィルタを含むサブジェクトです。 secureProv および secureCons は HTTPS フィルタを含むサブジェクトです。 この webCtrct コントラクトは、Web サービスを提供する EPG とそのサービスを消費するエンドポイントを含む EPG 間のセキュアな Web トラフィックと非セキュアな Web トラフィックの両方を可能にするために使用できます。

これらの同じ構造は、仮想マシンのハイパーバイザを管理するポリシーにも適用されます。 EPG が Virtual Machine Manager（VMM）のドメイン内に配置されると、APIC は EPG に関連付けられたすべてのポリシーを VMM ドメインに接続するインターフェイスを持つリーフ スイッチにダウンロードします。 VMM ドメインの完全な説明については、『ACI の基本』マニュアルの「Virtual Machine Manager のドメイン」の章を参照してください。 このポリシーが作成されると、APIC は EPG のエンドポイントへの接続を可能にするスイッチを指定する VMM ドメインにそれをプッシュ（あらかじめ入力）します。 VMM ドメインは、EPG 内のエンドポイントが接続できるスイッチとポートのセットを定義します。エンドポイントがオンラインになると、適切な EPG に関連付けられます。 パケットが送信されると、送信元 EPG および宛先 EPG がパケットから取得され、対応するコントラクトで定義されたポリシーでパケットが許可されたかどうかが確認されます。 許可された場合は、パケットが転送されます。 許可されない場合は、パケットはドロップされます。

コントラクトは、許可や拒否よりも複雑なアクションも許可します。 コントラクトは、所定のサブジェクトに一致するトラフィックをサービスにリダイレクトしたり、コピーしたり、その QoS レベルを変更したりできることを指定可能です。 具象モデルでアクセスポリシーをあらかじめ入力すると、APIC がオフラインまたはアクセスできない場合でも、エンドポイントは移動でき、新しいエンドポイントをオンラインにでき、通信を行うことができます。 APIC は、ネットワークの単一の障害発生時点から除外されます。 ACI ファブリックにパケットが入力されると同時に、セキュリティ ポリシーがスイッチで実行している具象モデルによって適用されます。

セキュリティ ポリシーの適用

トラフィックは前面パネルのインターフェイスからリーフ スイッチに入り、パケットは送信元 EPG の EPG でマーキングされます。 リーフ スイッチはその後、テナント エリア内のパケットの宛先 IP アドレスでフォワーディング ルックアップを実行します。 ヒットすると、次のシナリオのいずれかが発生する可能性があります。

1. ユニキャスト（/32）ヒットでは、宛先エンドポイントの EPG と宛先エンドポイントが存在するローカル インターフェイスまたはリモート リーフ スイッチの VTEP IP アドレスが提供されます。
2. サブネット プレフィクス（/32 以外）のユニキャスト ヒットでは、宛先サブネット プレフィクスの EPG と宛先サブネット プレフィクスが存在するローカル インターフェイスまたはリモート リーフ スイッチの VTEP IP アドレスが提供されます。
3. マルチキャスト ヒットでは、ファブリック全体の VXLAN カプセル化とマルチキャスト グループの EPG で使用するローカル レシーバのローカル インターフェイスと外側の宛先 IP アドレスが提供されます。

（注） マルチキャストと外部ルータのサブネットは、入力リーフ スイッチでのヒットを常にもたらします。 セキュリティ ポリシーの適用は、宛先 EPG が入力リーフ スイッチによって認識されるとすぐに発生します。

転送テーブルの誤りにより、パケットがスパイン スイッチの転送プロキシに送信されます。 転送プロキシはその後、転送テーブル検索を実行します。 これが誤りである場合、パケットはドロップされます。 これがヒットの場合、パケットは宛先エンドポイントを含む出力リーフ スイッチに送信されます。 出力リーフ スイッチが宛先の EPG を認識するため、セキュリティ ポリシーの適用が実行されます。 出力リーフ スイッチは、パケット送信元の EPG を認識する必要があります。 ファブリック ヘッダーは、入力リーフ スイッチから出力リーフ スイッチに EPG を伝送するため、このプロセスをイネーブルにします。 スパイン スイッチは、転送プロキシ機能を実行するときに、パケット内の元の EPG を保存します。

出力リーフ スイッチでは、送信元 IP アドレス、送信元 VTEP、および送信元 EPG 情報は、学習によってローカルの転送テーブルに保存されます。 ほとんどのフローが双方向であるため、応答パケットがフローの両側で転送テーブルに入力し、トラフィックが両方向で入力フィルタリングされます。

マルチキャストおよび EPG セキュリティ

マルチキャスト トラフィックでは、興味深い問題が起こります。 ユニキャスト トラフィックでは、宛先 EPG はパケットの宛先の検査からはっきり知られています。 ただし、マルチキャスト トラフィックでは、宛先は抽象的なエンティティ、マルチキャスト グループです。 パケットの送信元はマルチキャスト アドレスではないため、送信元 EPG は以前のユニキャストの例と同様に決定されます。 宛先グループの起源はマルチキャストが異なる場所です。

マルチキャスト グループが、ネットワーク トポロジから若干独立しているので、グループ バインディングへの (S, G) および (*, G) の静的設定は受け入れ可能です。 マルチキャスト グループが転送テーブルにある場合、マルチキャスト グループに対応するEPGは、転送テーブルにも配置されます。

（注） このマニュアルでは、マルチキャスト グループとしてマルチキャスト ストリームを参照します。

リーフ スイッチは、マルチキャスト ストリームに対応するグループを常に宛先 EPG と見なし、送信元 EPG と見なすことはありません。 前述のアクセス コントロール マトリクスでは、マルチキャストEPGが送信元の場合は行の内容は無効です。 トラフィックは、マルチキャスト ストリームの送信元またはマルチキャスト ストリームに加わりたい宛先からマルチキャスト ストリームに送信されます。マルチキャスト ストリームが転送テーブルにある必要があり、ストリーム内に階層型アドレッシングがないため、マルチキャスト トラフィックは、入力ファブリックの端でアクセスが制御されます。 その結果、IPv4 マルチキャストは入力フィルタリングとして常に適用されます。

マルチキャスト ストリームの受信側は、トラフィックを受信する前にマルチキャスト ストリームに最初に加わる必要があります。 IGMP Join 要求を送信すると、マルチキャスト レシーバは実際に IGMP パケットの送信元になります。 宛先はマルチキャスト グループとして定義され、宛先 EPG は転送テーブルから取得されます。 ルータが IGMP Join 要求を受信する入力点で、アクセス制御が適用されます。 Join 要求が拒否された場合、レシーバはその特定のマルチキャスト ストリームからトラフィックを受信しません。

マルチキャストEPGへのポリシーの適用は、前述のようにコントラクトのルールに従ってリーフ スイッチにより入力時に発生します。また、EPGバインディングに対するマルチキャスト グループは、APIC によって特定のテナント（VRF）を含むすべてのリーフ スイッチにプッシュされます。

タブー

セキュリティを確保する通常のプロセスも適用されますが、ACI ポリシー モデルは、どのようなセキュリティ プラクティスが採用されても完全性を確保するのに役立ちます。 ACI ポリシー モデルのアプローチでは、すべての通信がこれらの条件に準拠する必要があります。

- 通信は、モデルの管理対象オブジェクトであるコントラクトに基づいてのみ許可されます。コントラクトがなければ、EPG 間通信はデフォルトでディセーブルになります。
- ハードウェアへのダイレクト アクセスはなく、すべてのインタラクションはポリシー モデルを通じて管理されます。

タブーは、ネットワーク管理者がトラフィックの特定のクラスを拒否するために使用できるモデル内の特別なコントラクト管理対象オブジェクトです。 タブーは、パターンに一致するトラフィック（EPG、フィルタに一致する特定の EPG など）をドロップするために使用できます。 タブー ルールは、通常のコントラクトのルールが適用される前にハードウェアに適用されます。