コントラクトの使用

コントラクト

コントラクトは、Cisco Application Centric Infrastructure (ACI) 管理者にエンドポイント グループ間での Cisco ACI ファブリック内トラフィック フローを制御する手段を提供します。これらのコントラクトは、一方のエンドポイント グループが希望するサービスを提供し、もう一方のエンドポイント グループがそれらのサービスを消費するプロバイダー/コンシューマ モデルを使用して構築されます。コントラクトには、グローバル、テナント、VRF、またはアプリケーション プロファイルの範囲が割り当てられ、これによりコントラクトのアクセシビリティが制限されます。

つまり、コントラクトは 1 つ以上のサブジェクトで構成されます。各サブジェクトには 1 つ以上のフィルタが含まれます。各フィルタには 1 つ以上のエントリが含まれます。各エントリは、アクセス コントロール リスト（ACL）の 1 行に相当し、エンドポイント グループ内のエンドポイントが接続されているリーフ スイッチで適用されます。

詳細には、コントラクトは次の項目で構成されます。

- サブジェクト：特定のアプリケーションまたはサービス用のフィルタのグループ。
- フィルタ：レイヤ 2 ～ レイヤ 4 の属性 (イーサネット タイプ、プロトコル タイプ、TCP フラグ、ポートなど) に基づいてトラフィックを分類するために使用します。
- アクション：フィルタリングされたトラフィックで実行されるアクション。次のアクションがサポートされます。
  - トラフィックの許可 (通常のコントラクトのみ)
  - トラフィックのマーク (DSCP/CoS) (通常のコントラクトのみ)
  - トラフィックのリダイレクト (サービス グラフによる通常のコントラクトのみ)

- トラフィックのコピー(サービス グラフまたはSPANによる通常のコントラクトのみ)
- トラフィックのブロック（タブー コントラクトのみ）
- トラフィックのロギング（タブー コントラクトのみ）

- ラベル：（任意）ポリシーの適用における精度を高めるために、サブジェクトやエンドポイント グループなどのオブジェクトをグループ化するために使用します。

異なるエンドポイント グループは、定義済みのコントラクト ルールに基づいてのみ別のエンドポイント グループと通信できますが、エンドポイント グループ内通信ではコントラクトは必要ありません。同じエンドポイントグループ内のエンドポイント間のエンドポイントグループ内通信は、デフォルトで許可されます。

契約がサブジェクトと、2つのエンドポイント グループ（EPG）間の任意の送信元ポートと宛先ポート80を持つフィルタで定義されている場合、1つはコンシューマとして、もう1つはプロバイダーとして、Cisco ACI ファブリックはコンシューマ EPG からプロバイダー EPG へのパケットを許可します。宛先ポートは80、送信元ポートはanyです。ただし、プロバイダーからコンシューマへの戻りパケットはまだ許可されていません。リターンパケットを許可するオプションの1つは、フィルタのサブジェクトで **[両方の方向を適用（Apply Both Direction）]** と **[リバース フィルタ ポート（Reverse Filter Port）]** を有効にすることです。これら 2 つのオプションは、サブジェクトの作成時にデフォルトで有効になっています。

[両方の方向を適用（Apply Both Direction）] は、同じレイヤ 4 ポートの組み合わせを持つ反対方向のパケット、つまり、プロバイダー EPG から宛先ポート 80 および任意の送信元ポートを持つコンシューマ EPG へのパケットを許可するルールを作成します。次に、**[リバース フィルタ ポート（Reverse Filter Port）]** は、この新しいルールの宛先ポートと送信元ポートを反転させます。これにより、プロバイダー EPG からコンシューマ EPG へのパケットが、プロバイダー EPG からのリターンパケットと一致する宛先ポートと送信元ポート 80 で許可されるというルールが作成されます。

ただし、Cisco ACI コントラクトはステートフルではなく、プロバイダー EPG からコンシューマ EPG へのパケットはリターン パケットである必要はありません。これは、プロバイダー EPG がコンシューマ EPG へのトラフィックを開始する場合、送信元ポートが 80 であれば、Cisco ACI ファブリックはそれをすべての宛先ポートに許可することを意味します。フィルタの **[ステートフル（Stateful）]** オプションを使用すると、このような TCP トラフィックの問題を回避できます。**ステートフル** オプションが有効になっている場合、リターン方向（プロバイダーからコンシューマ）のルールは、TCP ポート（この例では宛先ポートと送信元ポート 80）の上にある TCP **ACK** フラグをチェックして、プロバイダーEPGから開始されたトラフィックをブロックします。

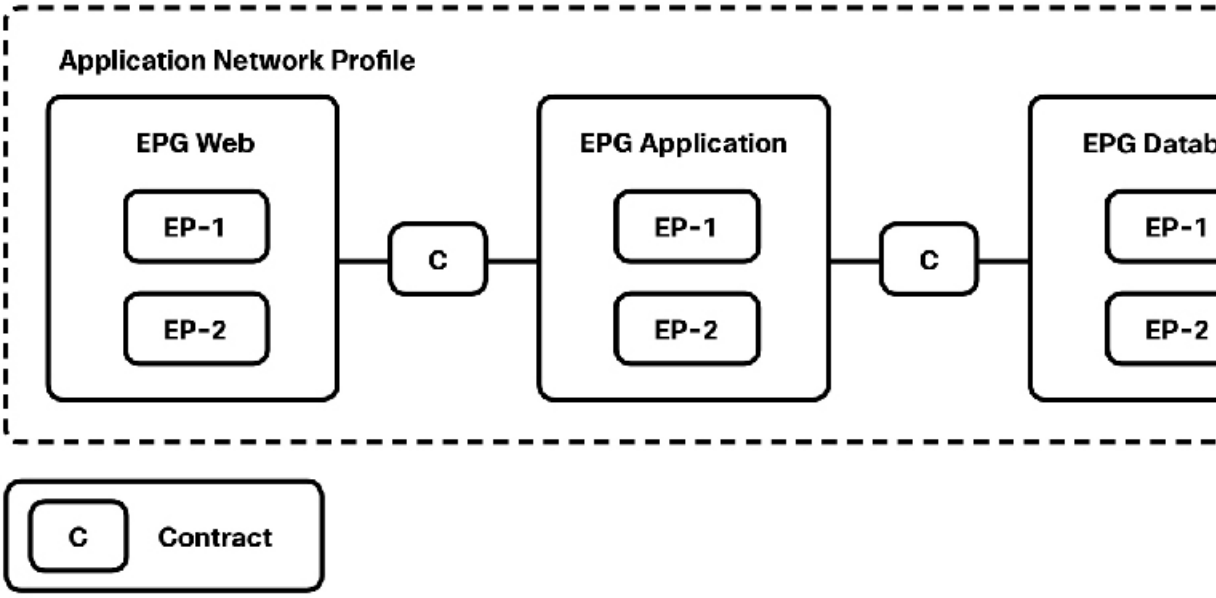
コントラクトを設定していない場合はマルチキャストキャストトラフィックおよび同一クラスのトラフィック以外に、次のタイプのパケットのトラフィックだけが許可されます。

- DHCP v4（prot 0x11、sport 0x44、dport 0x43）
- DHCP v4（prot 0x11、sport 0x43、dport 0x44）
- DHCP v6（prot 0x11、sport 0x222、dport 0x223）

- OSPF（prot 0x59）
- EIGRP（prot 0x58）
- PIM（prot 0x67）
- IGMP（prot 0x2）
- ND-Sol ICMPv6（prot 0x3a dport 0x0087）
- ND-Advt ICMPv6（prot 0x3a dport 0x0088）

次の例では、第 1 のエンドポイント グループ内の Web サーバ群、第 2 のエンドポイント グループ内のアプリケーション サーバ群、第3のエンドポイントグループ内のデータベース サーバ群を含む 3 層アプリケーションでのエンドポイント グループ間トラフィック フローを、さまざまなコントラクトが制御する方法を示します。Web エンドポイント グループ（プロバイダー）は、L3Outエンドポイント グループ（Cisco ACI ファブリックへの外部からのトラフィック）で使用されるコントラクト（contract1）を提供します。これにより、Cisco ACI ファブリックの外部から Web サーバに Web トラフィックが 到達できるようになります。アプリケーション エンドポイント グループ（プロバイダー）は、Web エンドポイント グループ（コンシューマ）が使用する通信用のコントラクト（contract2）を提供します。これにより、Web サーバはアプリケーションサーバ上のアプリケーションを呼び出せるようになります。最後に、アプリケーション エンドポイント グループ（コンシューマ）は、データベース エンドポイント グループ（プロバイダー）が提供するコントラクト（contract3）を使用します。これにより、アプリケーション サーバは、アプリケーションのデータベースにアクセスできるようになります。非確認済み UDP トラフィックの場合、リバース ポート フィルタリングは必要ありません。ただし、TCP トラフィックの場合は、応答側は、リバース ポート フィルタリングまたは応答側からのすべての確立されたトラフィックを許可する別のコントラクトがなければ TCP セッションを設定できません。

図 *1:* エンド ポイント グループ間のコントラクトポリシー



Cisco ACI で適用できるコントラクトの種類は次のとおりです。

- 通常のコントラクト
- タブー コントラクト
- アウトオブバンド（OOB）コントラクト

コントラクトは、次のタイプのエンドポイント グループの通信を管理します。

- アプリケーション エンドポイント グループ間
- アプリケーション エンドポイント グループと外部ネットワーク間
- アプリケーション エンドポイント グループとインバウンド向けのマネージメント エンドポイント グループ間。たとえば、インバウンドマネージメントが Cisco ACI ファブリック用に構成されており、特定のエンドポイントグループがそのファブリックへのアクセスを許可される場合などです。

アウトオブバンド コントラクトは、管理テナントからのアウトオブバンド トラフィックのみに適用されます。タブーコントラクトは、通常のコントラクトに関連するトラフィックを拒否およびロギングするために使用され、通常のコントラクトより前にハードウェア内に設定されます。たとえば、ポート 305 を除く送信元ポート 50 から 500 までのトラフィックを許可するには、タブーコントラクトにポート 305 を拒否する単一のエントリを作成し、一方、通常のコントラクトで 50 から 500 の範囲内のすべてのポートを許可します。ポート 305 を拒否するタブー コントラクトは、通常のコントラクトでポート 50 から 500 を許可する前に、ハードウェアにプログラムします。

コントラクト構成パラメータ

コントラクトを構成する場合は、次のオプションを定義できます。

- Application-profile：このコントラクトは、同じアプリケーション プロファイル内のすべてのエンドポイント グループに適用できます。
- Contract Scope：2 つ以上の参加ピア エンティティまたはエンドポイント グループ間のサービスコントラクトの範囲。コントラクトは、プロバイダー エンドポイント グループの範囲外のコンシューマ エンドポイント グループには適用されません。

  以下の状態があります。

  - **Private Network**：このコントラクトは、同じ VRF 内のすべてのエンドポイント グループに適用できます。
  - Tenant：このコントラクトは、同じテナント内のすべてのエンドポイント グループに適用できます。
  - Global：このコントラクトは、ファブリック全体にわたり、すべてのエンドポイント グループに適用できます。

  デフォルトのステータスは [Private Network] です。

- QoS Class：サービス コントラクトの優先度レベル。

  以下の優先度レベルを指定できます。

  - **[Unspecified]**
  - Level1：クラス 1 の DSCP（Differentiated Services Code Point）値。
  - Level2：クラス 2 の DSCP 値。
  - Level3：クラス 3 の DSCP 値。

  デフォルトは **Unspecified**（未指定）です。

- Tags (labels)：（任意）検索キーワードまたはアプリケーション プロファイルに割り当てられている用語。タグを使用すると、わかりやすい名前で複数のオブジェクトをグループ化できます。複数のオブジェクトに同じタグ名を割り当て、1 つのオブジェクトに 1 つ以上のタグ名を割り当てることができます。コントラクトがコンシューマまたはプロバイダーとしてエンドポイント グループに割り当てられている場合、デフォルトで、コントラクト内のすべてのサブジェクトがそのエンドポイント グループに適用されます。タグがある場合は、一致基準を持つアプリケーション プロファイル内のエンドポイント グループだけが、コントラクトのサブジェクトを導入します。

- Match：コンシューマ エンドポイント グループ間のサブジェクト一致基準。ラベルは、エンドポイント グループ、コントラクト、ブリッジ ドメイン、DHCP リレー ポリシー、および DNS ポリシーなどのさまざまなプロバイダーおよびコンシューマの管理対象オブジェクトに適用できます。プロバイダー ラベルとコンシューマ ラベルの一致を確認する場合、一致設定はプロバイダー エンドポイント グループによって決定されます。次のさまざまなオプションがあります。

- **AtleastOne**：少なくとも1つのラベルが、プロバイダー エンドポイント グループとコンシューマ エンドポイント グループで一致する。空白のラベルは一致と見なされます。
- AtmostOne：エンドポイント グループ上のすべてのラベルがまったく同じ場合にのみ一致する。空白のラベルは一致と見なされます。
- None：サブジェクト ラベルのいずれも一致しない。
- All：両エンドポイント グループに空白のラベル以外のすべてのラベルがある場合にのみ一致する。

デフォルトは **AtleastOne**（1 つ以上）です。

通常のコントラクトの作成/変更/削除

コントラクトの作成

1. メニュー バーで、**[Tenants]** > **[ALL TENANTS]** の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. ナビゲーション ウィンドウでは、***[Tenant_Name]*** > **[Security Policies]** > **[Contracts]** を選択します。
4. 作業ウィンドウで、**[Actions]** > **[Create Contract]**の順に選択します。
5. [Create Contract] ダイアログボックスで、次の操作を実行します。
    1. コントラクトの名前を入力します。
    2. （任意）コントラクト範囲を選択します。
    3. （任意）[QoS Class] を選択します。
    4. **[Subject]** の横にある **[+]** をクリックし、コントラクト サブジェクトを追加します。
        1. [Create Contract Subject] ダイアログボックスで、次の操作を実行します。
            1. コントラクトの件名を入力します。
            2. [Filter Chain] フィールドで [+] をクリックします。

               フィルタの作成については、「フィルタ」の項を参照してください。
6. **[更新（Update）]** をクリックします。
7. **OK** をクリックします。
8. [送信（Submit）] をクリックします。

コントラクトの変更

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Security Policies] > [Contracts] > *[Contract_Name]*** を選択します。
4. [Work] ペインで、[Policy] タブを選択します。
    1. （任意）[Contract Scope] を選択します。
    2. （任意）[QoS Class] を選択します。
    3. [Subject] フィールドの横にある [+] をクリックし、コントラクト サブジェクトを追加します。
        1. [Create Contract Subject] ダイアログボックスで、次の操作を実行します。
            1. コントラクトサブジェクトの**名前**を入力します。
            2. [Filter Chain] の横にある [+] をクリックします。

（注） フィルタの作成については、「フィルタ」の項を参照してください。

5. [Update] をクリックします。
6. [OK] をクリックします。
7. [送信（Submit）] をクリックします。

コントラクトの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Security Policies] > [Contracts] > *[Contract_Name]*** を選択します。
4. [Work] ペインで、[Actions] > [Delete] の順に選択します。

コントラクトの確認

```
REST :: /api/node/class/vzBrCP.xml

CLI :: moquery -c vzBrCP
```

EPG コントラクトの適用/削除

EPG へのコントラクトの適用

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Application Profiles]** > ***[Application_Profile_Name]*** > **[Application EPGs]** > ***[EPG_Name]*** > **[Contracts]** の順に選択します。
4. [Work] ペインで、[Actions] > [Add Provided Contract] または [Actions] > [Add Consumed Contract] を選択します。

   注：コントラクトの展開方法に応じた操作を選択します。
5. [Add Contract] ダイアログボックスで、次の操作を実行します。
   1. [Contract_Name] を入力します。
   2. [**QOS** policy] を選択します（任意）。
   3. [Label] を選択します（任意）。
6. [送信（Submit）] をクリックします。

EPG からのコントラクトの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Application Profiles]** > ***[Application_Profile_Name]*** > **[Application EPGs]** > ***[EPG_Name]*** > **[Contracts]** > ***[Contract_Name]*** の順に選択します。
4. [Work] ペインで、[Actions] > [Delete] の順に選択します。

EPG でのコントラクトの確認

```
Provider

REST :: /api/node/class/fvRsProv.xml

CLI :: moquery -c fvRsProv


Consumer

REST :: /api/node/class/fvRsCons.xml
```

```
CLI :: moquery -c fvRsCons
```

外部ネットワークコントラクトの適用/削除

外部ネットワークへのコントラクトの適用

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、 ***[Tenant_Name]*** > **[Networking] > [External Routed Networks] > *[Routed Outside_Name]* > [Networks] > *[External_Network_Instance_Profile]*** の順に選択します。
4. [Work] ペインで、[Add Provided Contract] または [Add Consumed Contract] のいずれかの横にある [+] をクリックします。

   注：コントラクトをどのように導入するかによって選択します。

   1. ***[Contract_Name]*** を選択します。
   2. [QOS Type] を選択します。
   3. [Match Criteria] を選択します。
5. [更新（Update）] をクリックします。

外部ネットワークからの通信に関するコントラクトの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、 ***[Tenant_Name]*** > **[Networking] > [External Routed Networks] > *[Routed Outside_Name]* > [Networks] > *[External_Network_Instance_Profile]*** の順に選択します。
4. 作業ウィンドウで、**[Contract_Name]** を選択し、 **[x]** をクリックします。

外部ネットワークコントラクトの確認

```
Provider

REST :: /api/node/class/fvRsProv.xml

CLI :: moquery -c fvRsProv


Consumer
```

```
REST :: /api/node/class/fvRsCons.xml

CLI :: moquery -c fvRsCons
```

VRF コントラクトの適用または削除

VRF インスタンス内のすべてのエンドポイント グループにコントラクトを適用するために、コントラクトを VRF インスタンスに直接適用できます。この概念は「vzAny」エンドポイント グループとも呼ばれます。単一の設定箇所から VRF インスタンス内のすべてのエンドポイントグループのコントラクトの設定を許可し、ハードウェアのリソース消費を最適化することでコントラクト管理を容易にします。

たとえば、Cisco Application Centric Infrastructure (ACI) 管理に 100 個のエンドポイント グループがあり、それらすべてが同じ VRF の部分である場合、エンドポイント グループごとではなく、VRF にあるこの 1 つの vzAny グループにコントラクトを適用できます。

VRF インスタンス規模のコントラクトとは、従来、TCP トラフィックで逆ポート転送をイネーブルにする必要なしに、エンドポイント グループ コントラクトが 1 方向（コンシューマからプロバイダー）のトラフィックのみを定義することを可能にする、確立されたトラフィックを許可するコントラクトです。VRF インスタンス内のすべてのエンドポイント グループが確立されたトラフィックを許可するため、エンドポイント グループに直接適用されるコントラクトで逆ポート転送は不要です。

コントラクトまたはその欠如が ACI ファブリックで VRF 内のトラフィックをブロックしているかを確認する簡便な方法として、VRF インスタンスを非強制化する方法があります。これにより、コントラクトを必要とせずに、VRF インスタンス内のすべてのエンドポイント グループ間の通信が許可されます。これは、VRF インスタンス エンドポイント グループに共通のテナント コントラクト vzAny を適用することに相当します。

（注） VRF 内に非常に多くのコントラクトがある場合は、VRF が強制化に戻ったときにリーフ スイッチにコントラクトを再導入するのに、最長で 1 時間かかる場合があります。

共有サービスの場合は、コンシューマ (vzAny) 側の宛先の pcTag（分類）を適切に導出するために、EPG の下にプロバイダ EPG 共有サブネットを定義する必要があります。コンシューマとプロバイダの両方のサブネットがブリッジ ドメイン下で定義され、共有サービス コンシューマとして機能する vzAny に対して、ブリッジ ドメインからブリッジドメインへの共有サービス設定から移行する場合は、少なくとも共有フラグを使用してプロバイダ サブネットを EPG に追加する追加の設定手順を実行する必要があります。

（注） 定義済みのブリッジ ドメイン サブネットの複製として EPG サブネットを追加する場合は、サブネットの両方の定義に同じフラグが定義されていることを確認してください。そうしないと、予期しないファブリック転送の動作が発生する可能性があります。

GUI を使用したコントラクトの VRF（vzAny）への適用

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Networking] > [Private Networks] >** ***[Private_Network_Name]*** > ***[EPG Collection for Context]*** の順に選択します。[
4. [Work] ペインで、[Add Provided Contract] または [Add Consumed Contract] のいずれかの横にある [+] をクリックします。

   コントラクトをどのように導入するかによって選択します。

   1. [Contract_Name] を入力します。
   2. [QOS Type] を選択します。
   3. [Match Criteria] を選択します。
5. [更新（Update）] をクリックします。

GUI を使用したコントラクトの VRF（vzAny）からの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Networking] > [Private Networks] >** ***[Private_Network_Name]*** > ***[EPG Collection for Context]*** の順に選択します。
4. 作業ウィンドウで、***[Contract_Name]*** を選択し、**[x]** をクリックします。

VRF コントラクトの確認

次の API は、VRF のコントラクトを確認します。

```
/api/node/class/vzBrCP.xml
```

次の iShell コマンドは VRF のコントラクトを確認します。

```
admin@apic1:~> moquery -c vzBrCP
```

フィルタ

フィルタは、トラフィックをフィルタリングするためのフィルタ エントリのグループです。各フィルタ エントリは、TCP/IP ヘッダー フィールド（レイヤ 3 プロトコル タイプ、レイヤ 4 ポートなど）に基づいて分類されるトラフィックを許可または拒否するのに使用されるルールです。フィルタは、エンドポイント グループに関連付けられるコントラクトで定義されます。エンドポイント グループに着信、エンドポイント グループから送信、またはその両方のいずれかに定義できます。サブジェクトは、フィルタをコントラクトに接続するエンティティで

す。エンティティは、このコントラクトにより提供されるかまたは消費されるエンドポイント間のトラフィックに影響を及ぼします。

フィルタ エントリ構成パラメータ

フィルタを構成する場合は、次のオプションを定義できます。

- **Name**：フィルタ エントリの名前。
- **EtherType**：フィルタ エントリの EtherType。次の EtherType があります。
  - 『**ARP**』
  - **FCOE**
  - **IP**
  - **MAC セキュリティ**
  - **MPLS Unicast**
  - **Trill**
  - **[Unspecified]**
- **ARP Flag**：フィルタ エントリのアドレス解決プロトコル フラグ。フィルタ エントリは、ネットワーク トラフィックの分類プロパティの組み合わせです。
- **IP Protocol**：フィルタ エントリの IP プロトコル。フィルタ エントリは、ネットワーク トラフィックの分類プロパティの組み合わせです。
- **Match Only Fragments**：パケット フラグメントにのみ一致。有効の場合、オフセットが 0 より大きいすべての IP フラグメント（最初のフラグメントを除くすべての IP フラグメント）にこのルールが適用されます。無効の場合、TCP/UDP ポート情報は最初のフラグメントでしかチェックできないため、オフセットが 0 より大きい IP フラグメントにルールは適用されません。
- Port Ranges (Source, Destination)：送信元と宛先のポート フィールド。[From] フィールドと [To] フィールドに同じ値を指定して単一のポートを指定するか、または、[From] フィールドと [To] フィールドに異なる値を指定して、0 ～ 65535 の範囲のポートを定義できます。数字を指定する代わりに、次のサーバタイプのいずれかを選択すると、事前定義されたタイプのポートを使用することができます。
  - **HTTPS**
  - **SMTP**
  - **[HTTP]**
  - **FTP-Data**
  - **[Unspecified]**
  - **[DNS]**

- **POP3**
- **rtsp**

デフォルトは **Unspecified**（未指定）です。

- **TCP フラグ**：このオプションは、EtherType、IPプロトコル、送信元ポート、および宛先ポートに加えて、トラフィックに一致するTCPフラグ値を指定します。使用可能なTCPフラグは次のとおりです。
  - **Synchronize**：SYN
  - **Established**：ACKまたはRST
  - **Acknowledgement**: ACK
  - **Reset**: RST
  - **Finish**: FIN
- **Stateful**：**Stateful**オプションは、**ACK**フラグが設定されている場合にのみ、プロバイダーからコンシューマへのTCPパケットを許可します。

GUI を使用したフィルタの作成

次の手順は、GUI を使用してフィルタを作成します。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[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 [Navigation] ペインで、**[Tenant *tenant_name*]** > **[Security Policies]** > **[Filters]** の順に選択します。

ステップ 4 [Work] ペインで、**[Actions]** > **[Create Filter]** の順に選択します。

ステップ 5 [Create Filter] ダイアログボックスで、次に指定されている点を除き、必要に応じてフィールドに入力します。

a) [Name] フィールドにフィルタの名前を入力します。
b) [Entries] テーブルの [+] をクリックします。

ステップ 6 [Entries] テーブルのフィールドに、次に指定するように入力します。

a) [Name] フィールドにフィルタ エントリの名前を入力します。
b) [Ethertype] ドロップダウン リストで、EtherType を選択します。
c) （任意） [ARP Flag] ドロップダウン リストで、ARP フラグを選択します。
d) （任意） [IP Protocol] ドロップダウン リストで、IP プロトコルを選択します。
e) （任意） 必要に応じて、[Match Only Fragments] チェックボックスにチェックマークを付けてください。
f) （任意） [Source Port From] ドロップダウン リストで、送信元ポートを選択します。

g) （任意） [Source Port To] ドロップダウン リストで、送信元ポートを選択します。
h) （任意） [Destination Port From] ドロップダウン リストで、宛先ポートを選択します。
i) （任意） [Destination Port To] ドロップダウン リストで、宛先ポートを選択します。
j) （任意） **[TCP Flags]** ドロップダウンリストで、TCPフラグを選択します。
k) （任意） 必要に応じて、**[Stateful]** チェックボックスをオンにします。
l) **Update** をクリックします。

ステップ 7 [送信（Submit）] をクリックします。

GUI を使用したフィルタの変更

次の手順は、GUI を使用してフィルタを変更します。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[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 [Navigation] ペインで、**[Tenant *tenant_name*]** > **[Security Policies]** > **[Filters]** > ***[filter_name]*** の順に選択します。
ステップ 4 [Navigation] ペインで、[Entries] テーブルの、変更するフィルタ エントリをダブルクリックします。
ステップ 5 値を変更します。
ステップ 6 [更新（Update）] をクリックします。

GUI を使用したフィルタの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、 ***[Tenant_Name]*** > **[セキュリティ ポリシー（Security Policies）] > [フィルタ（Filters）] > *[Filter_Name]*** を選択します。
4. [Work] ペインで、[Actions] > [Delete] の順に選択します。

NX-OS スタイルの CLI を使用したフィルタの設定

フィルタはテナント シェルを介して NX-OS スタイルの CLI で作成し、アクセスすることができます。

手順

ステップ 1 ファブリックの APIC に SSH 接続します。

```
# ssh admin@node_name
```

ステップ 2 設定モードを開始します。

```
apic1# configure
```

ステップ 3 目的のテナントに移動します。

```
apic1(config)# tenant tenant1
```

ステップ 4 「match tcp dest 80」と「match ip」のエントリを含む、「FilterHTTPS」と呼ばれるフィルタを作成します。

```
apic1(config-tenant)# access-list FilterHTTPS
 apic1(config-tenant-acl)# match tcp dest 80
 apic1(config-tenant-acl)# match ip
 apic1(config-tenant-acl)# exit
```

ステップ 5 「FilterHTTPS」フィルタを適用するコントラクトにアクセスします。

```
apic1(config-tenant)# contract WebHTTPS
```

ステップ 6 コントラクトにフィルタを接続するサブジェクト「SubjectHTTPS」を作成します。このようにして、同一のエントリを含む複数のフィルタを作成する必要なく、複数のコントラクトに同じフィルタを適用できます。

```
apic1(config-tenant-contract)# subject SubjectHTTPS
```

ステップ 7 フィルタをコントラクトに関連付けます。フィルタを使用して、コントラクト「WebHTTPs」に関連付けられているエンドポイントグループに入力しているトラフィックに一致させる、コントラクトに関連付けられているエンドポイントグループから出力しているトラフックに一致させる、またはその両方を行うことができます。

```
apic1(config-tenant-contract-subj)# access-group FilterHTTPS
 both  match traffic in both direction
 in    match traffic from provider to consumer
 out   match traffic from consumer to provider
apic1(config-tenant-contract-subj)# access-group FilterHTTPS both
```

NX-OS スタイルの CLI を使用したフィルタの削除

手順

ステップ 1 次のコマンドは、フィルタの関連付けを削除します。

```
apic1(config-tenant-contract-subj)# no access-group FilterHTTPS both
```

ステップ 2 次のコマンドは、すべてのフィルタを削除します。

```
apic1(config-tenant)# no access-list FilterHTTPS
```

フィルタの確認

フィルタを確認するには、次のいずれの方法も使用できます。

- GUI で、次の場所に移動します。

  [Tenant_Name] > **[Security Policies]** > **[Filters]** > ***[Filter_Name]***

- 次の API を使用します。

  ```
  /api/node/class/vzFilter.xml
  ```

- 次の NX-OS スタイルの CLI コマンドを入力します。

  ```
  apic1# show run
  ```

- 次のオブジェクト モデルの CLI コマンドを入力します。

  ```
  admin@apic1:~> moquery -c vzFilter
  ```

タブーコントラクト

ACI管理者が別のコントラクトによって許可されたトラフィックを拒否する必要がある場合があります。タブーコントラクトは、別のコントラクトによって許可される可能性がある特定のトラフィックを拒否するためにACI管理者が使用できる特殊なコントラクトです。タブーコントラクトは、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。タブーコントラクトのルールはハードウェアで通常のコントラクトのルールが適用される前の場合に適用されます。

従来のネットワーク概念を模倣するには、特定のタイプのトラフィックを制限するように構成したタブーコントラクトとともに、「すべてのトラフィックを許可する」コントラクトを適用します。

タブーコントラクト構成パラメータ

タブーコントラクトを構成する場合は、次のオプションを定義できます。

- **Name**：コントラクトまたはコントラクトのオブジェクトの名前。
- **Subjects**：ネットワーク ドメイン名のラベル。ラベルによって、互いに通信可能なオブジェクト、または通信できないオブジェクトを分類できます。
- **Directive**：タブー コントラクトに割り当てられたフィルタのディレクティブ。

タブー コントラクトの作成/変更/削除

タブーコントラクトの作成

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、 ***[Tenant_Name]*** **> [Security Policies] > [Taboo Contracts]** を選択します。
4. [Work] ペインで、[Actions] > [Create Taboo Contract] の順に選択します。
5. [Create Taboo Contract] ダイアログボックスで、次の操作を実行します。
   1. タブーコントラクトの**名前**を入力します。
   2. [Subject] フィールドの横にある [+] をクリックし、禁止サブジェクトを追加します。
      1. フィルタの**名前**を入力します。
      2. **ディレクティブ**を選択します。
6. [Update] をクリックします。
7. **OK** をクリックします。
8. [送信（Submit）] をクリックします。

タブーコントラクトの変更

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドで、 ***[Tenant_Name]*** **> [Security Policies] > [Taboo Contracts] >** ***[Taboo_Contract_Name]*** を選択します。
4. [Work] ペインで、[policy] を選択します。
   1. [Subject] フィールドの横にある [+] をクリックします。
   2. [Create Taboo Contract Subject] ダイアログ ボックスで、次の操作を実行します。
      1. タブー コントラクト サブジェクトの**名前**を入力します。
      2. [Filter Chain] フィールドで [+] をクリックします。
         1. フィルタの**名前**を入力します。
         2. **ディレクティブ**を選択します。

5. [送信（Submit）] をクリックします。

タブーコントラクトの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドで、 ***[Tenant_Name]*** > **[Security Policies] > [Taboo Contracts] > *[Taboo_Contract_Name]*** を選択します。
4. [Work] ペインで、[Actions] > [Delete] の順に選択します。

タブーコントラクトの確認

```
REST :: /api/node/class/vzTaboo.xml

CLI :: moquery -c vzTaboo
```

タブーコントラクトの適用/削除

EPG へのタブーコントラクトの適用

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、 ***[Tenant_Name]*** > **[Application Profiles] > *[Application_Profile_Name]* > [Application EPGs] > *[EPG_Name]* > [Contracts]** の順に選択します。
4. [Work] ペインで、[Actions] > [Add Taboo Contract] を選択します。
5. [Add Taboo Contract] ダイアログボックスで、次の操作を行います。
   1. **[Taboo** Contract] を選択します。
6. [送信（Submit）] をクリックします。

EPG からのタブーコントラクトの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、 ***[Tenant_Name]*** > **[Application Profiles] > *[Application_Profile_Name]* > [Application EPGs] > *[EPG_Name]* > [Contracts]** の順に選択します。

4. 作業ウィンドウで、[Taboo ***Contract_Name]*** > **[Actions]** > **[Delete]** の順に選択します。

EPG に適用したタブー コントラクトの確認

```
Provider

REST :: /api/node/class/fvRsProv.xml

CLI :: moquery -c fvRsProv


Consumer

REST :: /api/node/class/fvRsCons.xml

CLI :: moquery -c fvRsCons
```

テナント間コントラクト

ACI 管理者が 2 つのテナント間のトラフィックを許可する必要がある場合があります。インターフェイスコントラクトは、コントラクトのエクスポートを使用して特定のトラフィックを許可するためにACI管理者が使用できる特殊なタイプのコントラクトです。基本的に、コントラクトを送信元テナントでエクスポートし、ターゲットテナントにインポートします。従来のコントラクトと同様に、送信元 EPG はプロバイダー タイプです。ただし、ターゲット テナントでは、コントラクトはコントラクトインターフェイス タイプとしてインポートされます。一部の使用例には、次の章の完全なプロセスが示されています。

構成パラメータ

コントラクトをインポートする場合は、次のオプションを定義できます。

- Name：コントラクト インターフェイスの名前。
- Global Contract：2 つ以上の参加ピア エンティティ間で共有されるサービス コントラクトの名前。
- **Tenant**：ターゲットのエクスポートコントラクトのテナント名。

エクスポートコントラクトの作成/変更/削除

エクスポートコントラクト

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。

3. ナビゲーション ウィンドウでは、***[Tenant_Name]*** > **[Security Policies] > [Contracts]** を選択します。
4. [Work] ペインで、[Actions] > [Export Contract] の順に選択します。
5. [Export Contract] ダイアログボックスで、次の操作を実行します。
   1. エクスポートコントラクトの**名前**を入力します。
   2. [Global Contract] を選択します。
   3. [Tenant Name] を入力します。
6. [完了（Finish）] をクリックします。

エクスポートされたコントラクトの変更

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Security Policies] > [Contracts] >** ***[Contract_Name]*** を選択します。
4. [Work] ペインで、[policy] を選択します。
   1. エクスポートコントラクトの**名前**を入力します。
   2. [Global Contract] を選択します。
   3. [Tenant Name] を入力します。
5. [完了（Finish）] をクリックします。

エクスポートされたコントラクトの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、***[Tenant_Name]*** > **[Security Policies] > [Contracts] > [Imported Contracts] >** ***[Contract_Name]*** の順に選択します。
4. [Work] ペインで、[Actions] > [Delete] の順に選択します。

エクスポートされたコントラクトの確認

```
REST :: /api/node/class/vzCPif.xml

CLI :: moquery -c vzCPif
```

入力ベース ACL

入力ベースACL機能の主な目的は、境界リーフのリソースを節約することです。このポリシー拡張モデルでは、ポリシーは非境界リーフのみに適用されるため、境界リーフでのゾーンルールの使用量が低減します。このポリシーの適用方向はVRF レベルで適用され、前のポリシーの適用との下位互換性が許可されます。この新しいモデルのポリシーが適用方向は次のとおりです。

1. Host to WAN：ポリシーは非境界リーフで適用されます。
2. WAN to Host：ポリシーは、エンドポイント グループが境界リーフで既知であるかにかかわらず、非境界リーフで適用されます。
3. WAN to WAN：ポリシーは入力境界リーフで適用されます。

この機能は、中継ルーティング、vzAny、タブー コントラクトの使用例とは互換性がありません。中継ルーティング規則はすでに入力に適用されています。

GUI を使用した入力ベース ACL の設定

ポリシー コントロールの適用の方向は VRF で適用されます。

手順

ステップ 1 メニュー バーで、**[Tenant]** > **[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 [Navigation] ペインで、**[Networking]** > **[VRFs]** > **[VRF Name]** の順に選択します。
ステップ 4 [Work] ペインで、[Policy Control Enforcement Direction] を [Ingress] に設定します。
ステップ 5 [Submit] をクリックします。`
ステップ 6 ポリシーの使用を確認し、[Submit Changes] をクリックします。

入力ベース ACL の確認

次の iShell コマンドは入力ベースの ACL を確認します。

```
admin@apic1:~> moquery -c fv.Ctx -f 'fv.Ctx.name=="vrf-name"'
```

次のハードウェア CLI コマンドは入力ベースの ACL を確認します。

```
# vsh_lc
module-1# show system internal eltmc info vrf name
```

コントラクトの使用例

これらの使用例はすべて、EPG-1 のホストが EPG-2 のホストと通信して双方向トラフィックを実現することが目的であると想定しています。これらのシナリオがどのように実現されるかは、選択した運用モデルや、システムがオブジェクトの再利用を重視しているのか、テナント

の自立性を重視しているのかによって異なります。詳細な説明については、コントラクトのスコーピングに関するコントラクトの項を参照してください。

次に、いくつかの一般的なシナリオを示します。

1. テナント間コントラクト
2. プライベート ネットワーク間コントラクト
3. リバースフィルタを使用した双方向通信の単一コントラクト
4. 複数フィルタを使用した単一方向の単一コントラクト
5. 単一フィルタを使用した単一方向の複数コントラクト

テナント間コントラクト

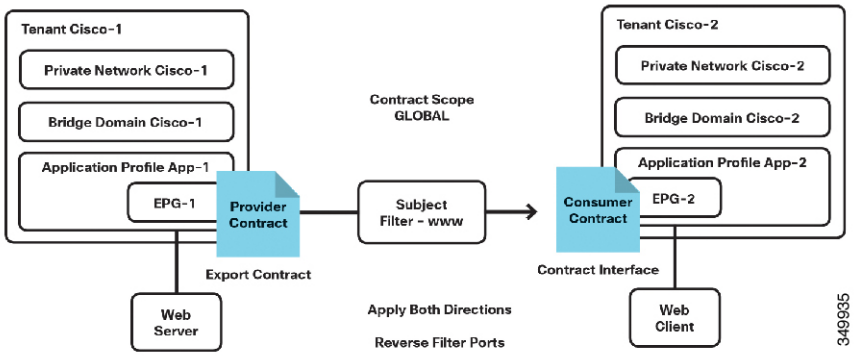
ACME 社は、ほとんどの企業と同様に、名前解決に DNS、ユーザ管理に Active Directory という具合に、共有サービスを利用しています。テナントのほとんどがこれらのサービスを使用する予定であるため、ACME 社 ではファブリック全体でこのトラフィックを許可する必要があります。異なるテナントに所属している EPG 間の通信は、同じコントラクトを共有している場合にだけ許可されます。同じコントラクトを使用するには、送信元のテナントから適切な接続先のテナントにそのコントラクトをエクスポートする必要があります。コントラクトは、接続先のテナントの [Security Policies] の [Imported Contract] セクションの下に表示されます。

使用されたコントラクトのインターフェイスを使用して、接続先のテナントの EPG とインポートされたコントラクトを関連付けます。

注：コントラクト消費のインターフェイスは、コントラクトで定義されている 1 つ以上のサブジェクトを表します。インターフェイスに関連付けることで、エンドポイント グループはインターフェイスによって示されるすべてのサブジェクトの使用を開始します。

次の使用例では、テナント Cisco-1 の EPG-1 にはテナント Cisco-2 の EPG-2 との通信が必要です。これは、連絡先インターフェイスを利用すると実現されます。テナント Cisco-1 では、ユーザが目的のコントラクトインターフェイスをエクスポートします。テナント Cisco-1 で、ユーザは目的のコントラクトをエクスポートし、EPG-2 にコントラクトを提供するプロバイダーを選択します。次に、ユーザは、テナント Cisco-2 にインポートされたコントラクトを確認し、使用するコントラクトとしてそのコントラクトを選択します。発信元 VRF から目的の VRF へのルートをアドバタイズするには、EPG 内にサブネットを作成する必要があります。

図 *2:* テナント間でのコントラクトのエクスポート



テナント Cisco-1/EPG-1

1. [Security Policies] で [Export Contract] を作成します。
2. EPG1 の**共有**サブネット範囲にホスト サブネット（デフォルトのゲートウェイ IP）を作成します。
3. EPG1 の**プロバイダー** コントラクト タイプにコントラクトを追加します。
4. ブリッジ ドメインの**プライベート/パブリック**のサブネット範囲にホスト サブネットを作成します。

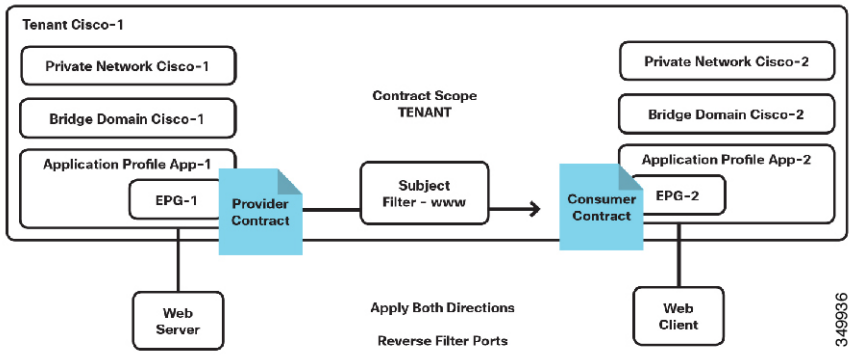
テナント Cisco-2/EPG-2

1. エクスポートしたコントラクトが [Imported Contracts] に表示されていることを確認します。
2. EPG2 の**共有**サブネット範囲にホスト サブネット（デフォルトのゲートウェイ IP）を作成します。
3. EPG2 の**使用される**コントラクト タイプにインターフェイス コントラクトを追加します。
4. ブリッジ ドメインの**プライベート/パブリック**のサブネット範囲にホスト サブネット（デフォルトのゲートウェイ IP）を作成します。

プライベート ネットワークコントラクトの通信

次の使用例では、VRF Cisco-1 の EPG-1 には VRF Cisco-2 の EPG-2 との通信が必要です。これは、EPG 内のサブネット フィールドを利用することで実現されます。EPG にサブネットを作成し、共有を選択することで、テナントを対象とするコントラクト内に示された VRF にルートがリークされます。

図 *3:* プライベート ネットワーク間でのコントラクトのエクスポート



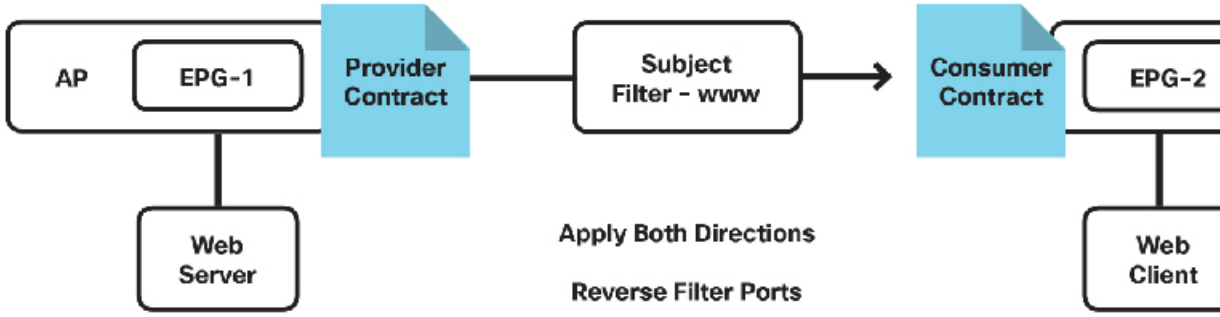
1. [Security Policies] でコントラクトスコープを [Tenant] としてコントラクトを作成します。
2. （テナント Cisco-1/EPG-1）**EPG1** の共有サブネット範囲にホスト サブネット（デフォルトのゲートウェイ IP）を作成します。
3. **EPG1** のプロバイダー コントラクト タイプにコントラクトを追加します。
4. （テナント Cisco-1/EPG-2）**EPG2** の共有サブネット範囲にホスト サブネット（デフォルトのゲートウェイ IP）を作成します。
5. **EPG2** のプロバイダー コントラクト タイプにコントラクトを追加します。

単一コントラクト、双方向、逆フィルタ

この使用例は、両方向にコントラクトサブジェクトを適用するオプションと、フィルタ処理リバースを適用するオプションのコントラクトを実装する場合に役に立ちます。これは、最も一般的な使用例であり、単一プロバイダー/コンシューマ関係で実装する単一サブジェクト/フィルタを考慮しています。

次の使用例では、EPG-1は、「www」という名前のサブジェクトとのコントラクトを提供します。このサブジェクトには、送信元ポート any および宛先ポート 80（HTTP）を使用する TCP トラフィック用のフィルタと、**[Apply Both Direction]** および **[Reverse Filter Port]** オプションがあります。 これにより、EPG-2 の Web クライアントは EPG-1 の Web サーバのポート 80 で HTTP セッションを開始できます。つまり、EPG-1 は EPG-2 にサービスを提供しています。ただし、これにより、EPG-1 はポート 80 から EPG-2 の任意のポートへの TCP セッションを開始できます。これは通常、設定の目的ではありません。同じフィルタで**ステートフル**オプションを有効にすると、EPG-1（プロバイダー）からの **TCP ACK** フラグを持つトラフィックのみが許可され、トラフィックが最初にコンシューマ側から開始されるようになります。ただし、ステートフル ファイアウォールとは異なり、プロバイダーからの SYN + ACK 攻撃は防止されません。

図 *4:* 逆のフィルタを使用したデフォルトの双方向コントラクト



結果：

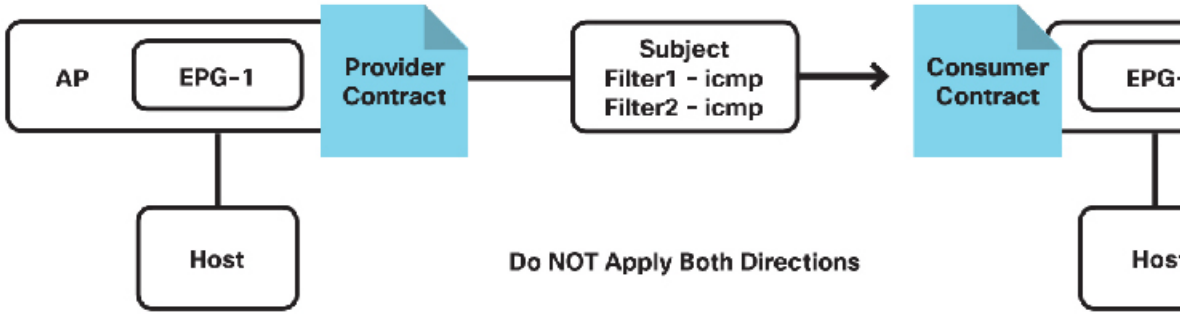
1 つのサブジェクトと、単一プロバイダーと単一コンシューマの 1 つのフィルタによる単一コントラクト。この例では、www です。

複数フィルタを使用した単一方向の単一コントラクト

この使用例には、両方向にコントラクトサブジェクトを適用するオプションなしでのコントラクトの実装が含まれています。このオプションを選択すると、逆フィルタ オプションを選択するオプションがなくなります。

次の使用例では、EPG-1 がサブジェクト icmp のコントラクトを提供し、EPG-2 がそのコントラクトを使用します。これにより、EPG-1 のホストは icmp を介してい EPG-2 のホストにアクセスできます。単一サブジェクトを [Apply Both Directions] を使用せずに利用すると、各方向に 1 つずつ、2 つのフィルタを構成する必要があります。

図 *5*: 単一コントラクト、単一の単一方向サブジェクト、複数フィルタ



結果：

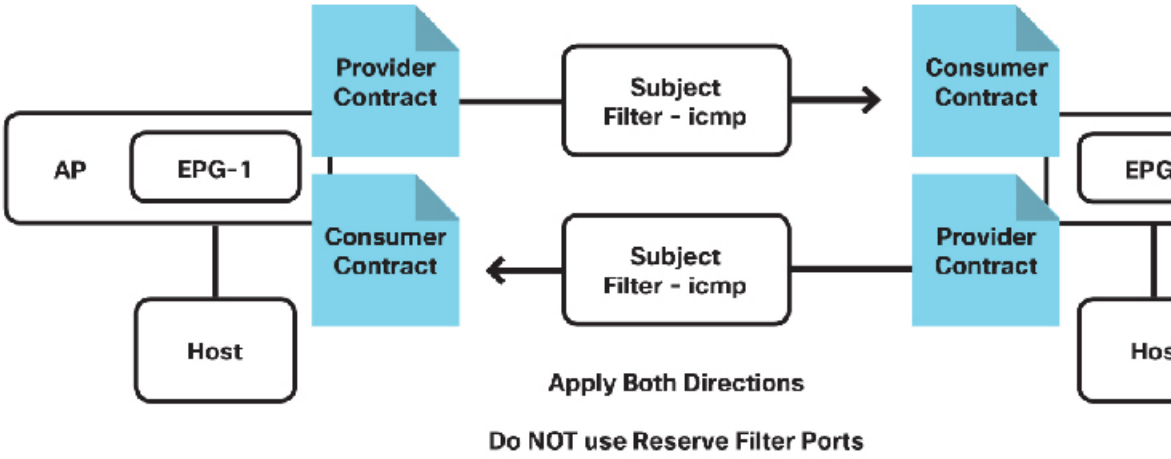
（1）サブジェクトと（2）フィルタによる単一のコントラクトと単一プロバイダーおよび単一コンシューマ。この例では、icmp です。

単一方向単一フィルタの複数コントラクト

この使用例は、両方向にコントラクトサブジェクトを適用するオプションをフィルタ処理フィルタを適用するオプションを使用せずにコントラクトを実装する場合に役に立ちます。これにより、エンドユーザはコントラクト導入時に最も高い粒度を許可できますが、最も包括的にもなります。

次の使用例では、EPG-1 はサブジェクト www のコントラクトを提供し、EPG-2 はそのコントラクトを使用します。これにより、EPG-2 の Web クライアントが EPG-1の Web サーバにアクセスできます。つまり、EPG-1 は EPG-2 にサービスを提供しています。

図 *6*: 複数のコントラクト、単一方向サブジェクト、単一フィルタ



結果：

（1）サブジェクト（1）フィルタを使用した2つのコントラクト。各コントラクトに同じコントラクトを参照する単一プロバイダーと単一コンシューマがあります。ここで異なるのは、コントラクトが双方向に明示的に適用されることです。