アトミック カウンタ ポリシーの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[設定](#)
[設定するアトミックポリシーのタイプの決定](#)
[ポリシーの作成](#)
[EPからEP](#)
[EPGからEPG](#)
[EPからEPG](#)
[EPから外部](#)
[EPGからEP](#)
[EPGからIP](#)
[IPの外部](#)
[IPからEPG](#)
[ポリシーに使用するフィルタの追加](#)
[確認](#)
[トラブルシュート](#)

概要

このドキュメントでは、アトミックカウンターポリシーがファブリックでどのように機能するかを説明します。この機能を使用すると、ファブリック上のトラフィックドロップ/超過パケットを監視できます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- シスコアプリケーションセントリックインフラストラクチャ(ACI)
- APICバージョン1.0(3n)
- n9000-aciバージョン11.0(3n)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています

。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

この記事では、次の略語を使用しています。

- APIC:Application Policy Infrastructure Controller（アプリケーションポリシーインフラストラクチャコントローラ）
- TEP：トンネルエンドポイント
- VRF:Virtual Routing & Forwarding
- TCAM:Ternary Content-Addressable Memory(TCAM)
- EPG：エンドポイントグループ
- MO – 管理対象オブジェクト

「トラブルシューティング」セクションには、トピックの理解に役立つ重要な情報がいくつかあります。最も重要な点は、アトミックカウンタポリシーをすべて活用するために、測定されるトラフィックがファブリック(leaf > spine > leaf)を通過する必要があることです。同じリーフに接続されている2つのエンドポイントに対してポリシーを作成すると、送信カウンタの増加のみが許可されます。

アトミックカウンタには複数のタイプがあることに注意してください。このドキュメントでは、オンデマンドのアトミックカウンタポリシーを設定する方法について説明します。これらは、管理者がオンまたはオフを切り替えることができます。また、リーフ間のトラフィックを測定する「常時接続」のアトミックカウンタもあります。これらはTEP-to-TEPアトミックカウンタです。次の項目で確認できます。

- dbgIngrTep（入力TEPカウンタ）
- dbgEgrTep（出力TEPカウンタ）

各リーフのTEPごとにカウントされます。これらの番号に対してApplication Policy Infrastructure Controller(APIC)をポーリングすることは可能ですが、推奨されません。ネットワーク上のトラフィックの監視に関心のあるお客様に対する最善の対策は、オンデマンドカウンタの設定です。

動作するために、アトミックカウンタはeVXLANヘッダーの「M」ビットをオンまたはオフにします。時間に関しては増加せず、「パケット」に関しては増加します。 Mビットは、パケットに対して増加するバンク（奇数または偶数）をノードに伝えます。アトミックカウンタは、それぞれのオッドおよび偶数バンクのカウンタのノードをポーリングすることによって動作します。たとえば、APICは、オンデマンドポリシーが設定されているため、リーフ1のオッドバンクとリーフ4の偶数バンクを測定できます。これにより、APICは各バンクカウントから送信パケットと受信パケットを取得し、その差に基づいて廃棄パケットと超過パケットの数を算出できます。

オンデマンドポリシーが設定されている場合、TCAMエントリが一致し、奇数/偶数ビットが設定されると、カウンタが増加します。つまり、アトミックカウンタが機能するには、測定しようとする2つのエンドポイント/エンドポイントグループ/IP間のコントラクトを介してポリシーを設定する必要があります。

アトミックポリシーカウンタを設定する際に考慮すべき注意点を次に示します。

- エンドポイントが異なるテナントまたは同じテナント内の異なるコンテキスト(VRF)にある場合、アトミックカウンタの使用はサポートされません。
- IPアドレスが学習されない純粋なレイヤ2設定(IPアドレスは0.0.0.0)では、エンドポイントか

らEPGおよびEPGからエンドポイントへのアトミックカウンタポリシーはサポートされません。このような場合、エンドポイント間ポリシーとEPG間ポリシーがサポートされます。外部ポリシーは、学習されたIPアドレスを必要とする仮想ルーティングおよび転送(VRF)ベースであり、サポートされています。
- アトミックカウンタの送信元または宛先がエンドポイントである場合、エンドポイントは静的ではなく動的である必要があります。ダイナミックエンドポイント(fv:CEp)とは異なり、スタティックエンドポイント(fv:StCEp)には、アトミックカウンタに必要な子オブジェクト(fv:RsCEpToPathEp)がありません。
- トランジットトポロジでは、リーフスイッチがすべてのスパインスイッチとフルメッシュ状態になく、リーフ間（TEPからTEP）カウンタが期待どおりに動作しません。
- リーフ間（TEPからTEP）アトミックカウンタでは、トンネルの数がハードウェア制限を増やした後、システムによってモードがトレールモードからパスモードに変更され、スパイン単位のトラフィックは表示されなくなります。
- アトミックカウンタはスパインプロキシトラフィックをカウントしません。
- パケットがファブリックに入る前、またはリーフポートに転送される前にドロップされたパケットは、アトミックカウンタでは無視されます。
- ハイパーバイザ（同じポートグループとホスト）でスイッチングされたパケットはカウントされません。
- アトミックカウンタには、アクティブなファブリックネットワークタイムプロトコル(NTP)ポリシーが必要です。
- 送信元および/または宛先としてfvCEpが設定されたアトミックカウンタポリシーは、fvCEp管理対象オブジェクト(MO)に存在するMACアドレスおよびIPアドレスとの間のトラフィックのみをカウントします。 fvCEp MOに空のIPアドレスフィールドがある場合、そのMACアドレスとの間のすべてのトラフィックは、IPアドレスに関係なくカウントされます。APICが1つのfvCEpに対して複数のIPアドレスを学習した場合、fvCEp MO自体の1つのIPアドレスからのトラフィックだけが前述のようにカウントされます。特定のIPアドレスとの間でアトミックカウンタポリシーを設定するには、送信元または宛先としてfvIp MOを使用します。
- fvCEpの背後にfvIpがある場合、fvCEpベースのポリシーではなく、fvIPベースのポリシーを追加する必要があります。

詳細は、『Cisco APICトラブルシューティングガイド – アトミックカウンタのガイドラインと制限』を参照してください。

設定

アトミックカウンタポリシーを設定するには、次の手順を実行します。

1. 設定するアトミックカウンタポリシーのタイプを決定します。
2. ポリシーを作成します。
3. ポリシーに使用するフィルタを追加します。

設定するアトミックポリシーのタイプの決定

次のタイプのオンデマンドアトミックカウンタポリシーを設定できます。

- EPからEP
- EPからEPG

- EPから外部
- EPGからEP
- EPGからEPG
- EPGからIP
- IPの外部
- IPからEPG

各略語の意味は次のとおりです。

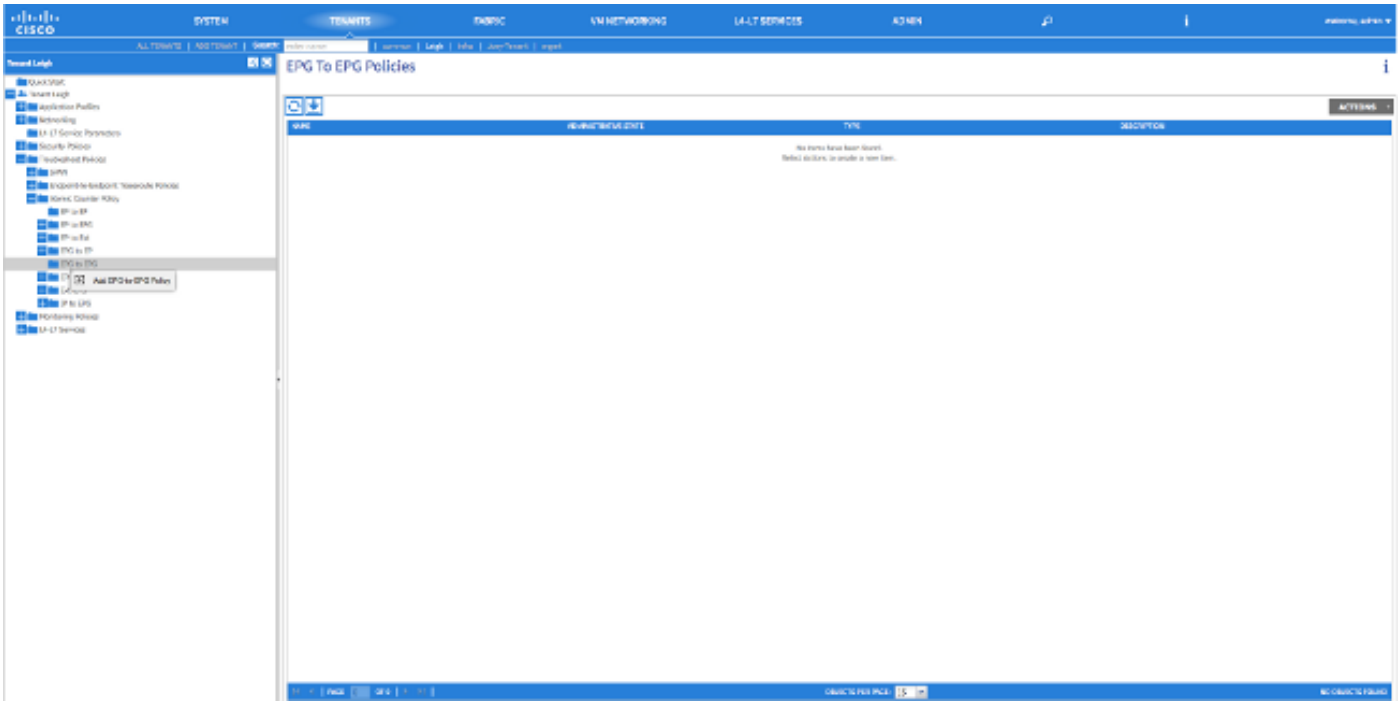
- EP – エンドポイント
- EPG：エンドポイントグループ
- 外部 – 外部ネットワーク
- IP:IPアドレス

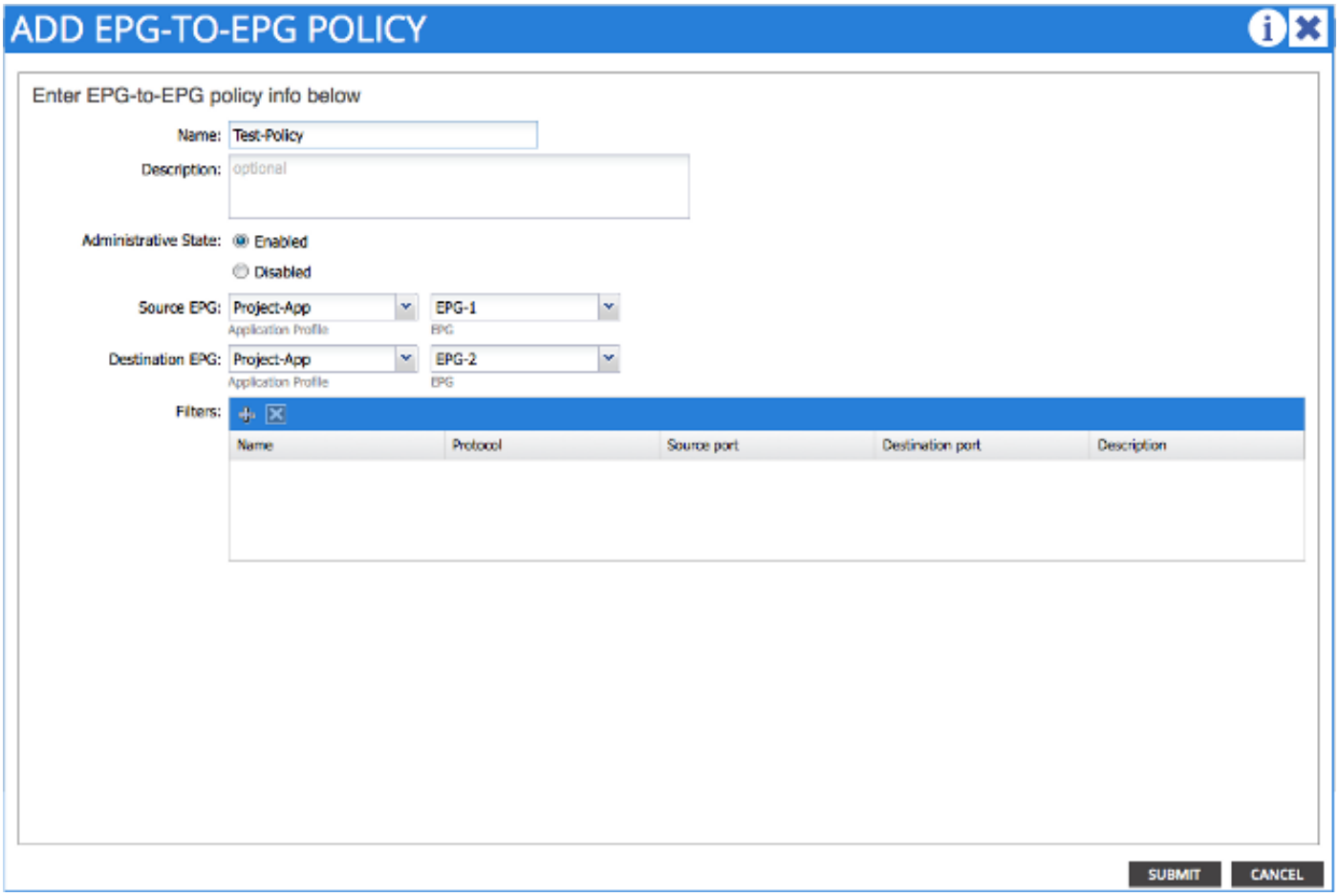
EPベースのポリシーでは、ポリシーを設定する前に、エンドポイントをファブリックで学習しておく必要があります。

設定するポリシーのタイプによって、次のセクションで設定する必要があるパラメータが決まります。

ポリシーの作成

このセクションで使用するスクリーンショットは、EPGからEPGへのポリシー用です。設定するタイプによってビューが異なる場合がありますが、コアコンセプトは同じです。





EPからEP

次の2つのソースタイプから選択できます。EPとIP。[EP]を選択した場合は、ファブリックで学習されたエンドポイントを選択します。[IP]を選択した場合は、ファブリックで学習されたエンドポイントとIPアドレスを選択します。これにより、特定のエンドポイントと、エンドポイントの背後に位置する可能性のある特定のIPホストを決定する際に、より詳細な情報を得ることができます。

EPGからEPG

ポリシーの送信元および宛先EPGを選択します。これにより、送信元EPGのすべてのエンドポイントから宛先EPGのすべてのエンドポイントに送信されるトラフィックが測定されます。

EPからEPG

ソースを選択するプロセスは、「EP to EP」ポリシーのプロセスと同じです。宛先を選択するプロセスは、「EPGからEPGへ」ポリシーと同じです。

EPから外部

ソースを選択するプロセスは、「EP to EP」ポリシーのプロセスと同じです。カウンタの宛先として使用されるファブリック外のIPアドレスを指定するには、「External IP」を入力する必要があります。アドレスの後に「/」を付け、サブネットサイズを指定することで、特定のIPアドレスまたはIPアドレス範囲を1つ選択できます。

EPGからEP

ソースを選択するプロセスは、「EPGからEPGへ」ポリシーと同じです。宛先を選択するプロセスは、「EP to EP」ポリシーのプロセスと同じです。

EPGからIP

ソースを選択するプロセスは、「EPGからEPGへ」ポリシーと同じです。宛先を選択するプロセスは、「EP to Ext」ポリシーと同じです。

IPの外部

トラフィックの送信元IPアドレスを選択し、[Source IP]フィールドに入力します。特定のIPアドレスまたはIPサブネットのいずれかになります。宛先を選択するプロセスは、「EPからEP」ポリシーと同じです。

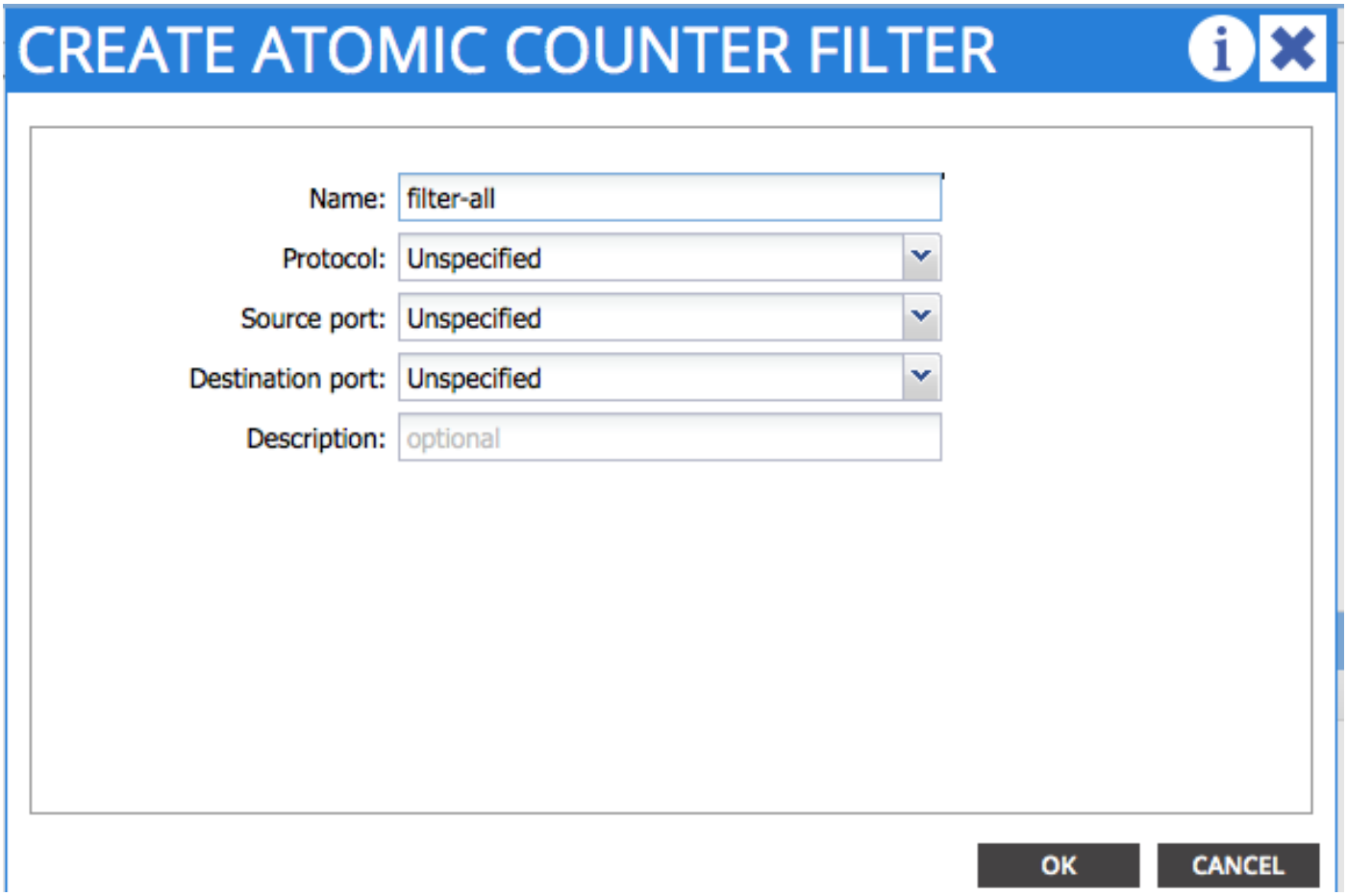
IPからEPG

送信元を選択するプロセスは、「Ext to IP」ポリシーと同じです。宛先を選択するプロセスは、「EPGからEPGへ」ポリシーと同じです。

ポリシーに使用するフィルタの追加

ここに表示される画面は、設定するポリシーのタイプに関係なく一貫しています。アトミックカウンタフィルタは、ファブリック内のコントラクトに適用するフィルタとは異なるタイプのオブジェクトですが、同様の機能を備えています。

- [名前]：アトミックカウンタフィルタの名前をここに入力します。このフィルタは、このポリシーのみに固有であり、再利用されないことに注意してください。
- プロトコル：ドロップダウンリストからプロトコルを選択するか、0 ~ 255のプロトコルに対応する番号を入力します。0 ~ 255の範囲は、IPパケットヘッダーに含まれるIPプロトコル番号に対応します。
- 送信元ポート：ドロップダウンリストから一般的に使用されるプロトコルを1つ選択するか、0 ~ 65535の数値を入力できます。
- 宛先ポート：ドロップダウンリストから一般的に使用されるプロトコルを1つ選択するか、0 ~ 65535の数値を入力できます。
- [説明(Description)]：これは、識別に役立つフィルタの説明です。このフィルタによって識別されるトラフィックまたは識別されないトラフィックには影響しません。



REST APIを使用してアトミックカウンタを設定することもできます。EPGからEPGへのポリシーの作成に使用されるPOST要求の例を次に示します。

URL:https:// **<apic-ip>** /api/node/mo/uni/tn-Leigh/epgToEpg-Test-Policy.json

JSON

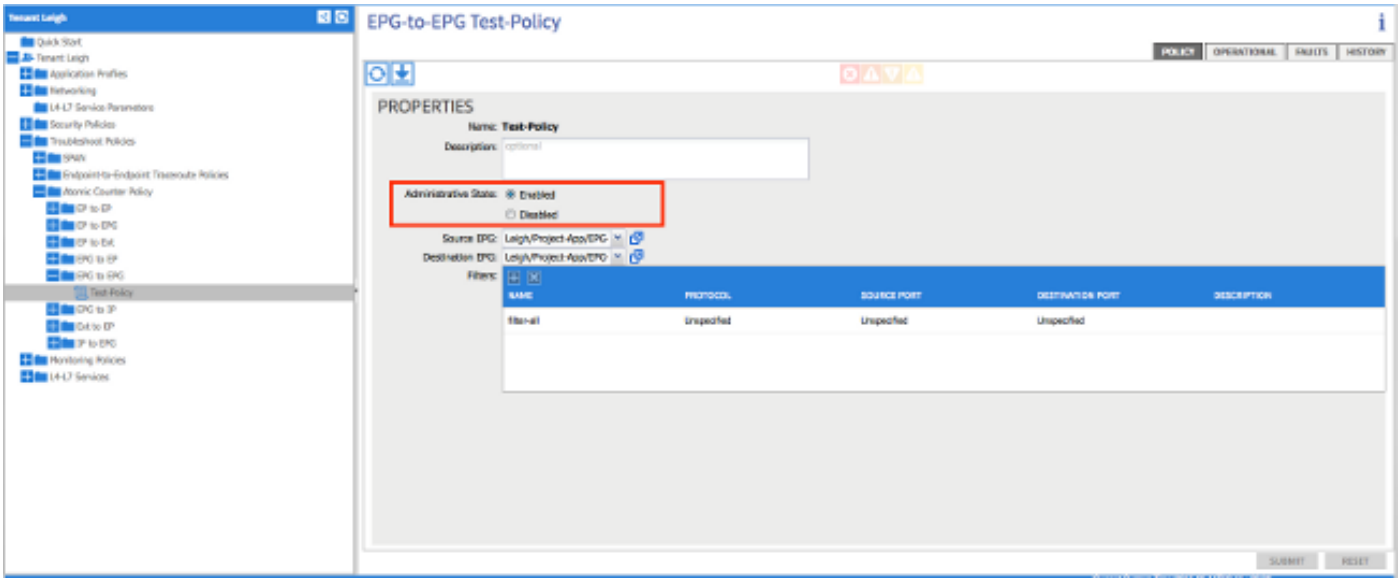
```
{"dbgacEpgToEpg":
   {"attributes":
       {"dn":"uni/tn-Leigh/epgToEpg-Test-Policy",
       "name":"Test-Policy",
       "rn":"epgToEpg-Test-Policy",
       "status":"created"},
       "children":[
            {"dbgacFilter":
                {"attributes":
                    {"dn":"uni/tn-Leigh/epgToEpg-Test-Policy/filt-filter-all",
                    "name":"filter-all",
                    "rn":"filt-filter-all",
                    "status":"created"},
                    "children":[]}},
            {"dbgacRsFromEpg":
                {"attributes":
                    {"tDn":"uni/tn-Leigh/ap-Project-App/epg-EPG-1",
                    "status":"created,modified"},
                    "children":[]}},
            {"dbgacRsToEpgForEpgToEpg":
                {"attributes":
                    {"tDn":"uni/tn-Leigh/ap-Project-App/epg-EPG-2",
                    "status":"created"},
                    "children":[]
```

```
                }
            }
        ]
    }
}
```

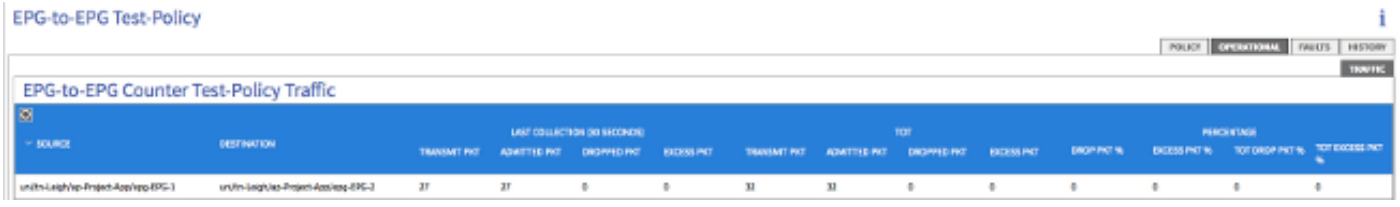
確認

ここでは、設定が正常に機能しているかどうかを確認します。

設定したアトミックカウンタポリシーが動作可能であることを確認する最も簡単な方法は、[Policy]タブで[Administrative State]が[Enabled]に設定されていることを確認することです。



ポリシーの各統計情報のカウンタを表示するには、[Operational]タブに移動します。トラフィックが流れると、送信パケットと許可パケットの数が増加します。1％以上のパケットが廃棄されるとマイナー障害がトリガーされ、5％以上のパケットが廃棄されるとメジャー障害がトリガーされます。



トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

カウンタが増加していない場合は、次のような問題が発生する可能性があります。

- ポリシーは有効になっていますか。
- ポリシーのフィルタは正しく設定されていますか。
- 2つのエンドポイント間またはデバイス間でトラフィックを測定する契約は存在しますか。

ポリシーが正しく設定され、有効になっており、テスト対象のエンドポイントがトラフィックを正常に渡す場合、問題は2つのエンドポイントが同じリーフに接続されている可能性があります。ハードウェアアーキテクチャの設計により、カウンタが増加するためには、リーフ上のノースス

ターASICをトラフィックが通過する必要があります。トラフィックが1つのリーフのみを通過する場合は、送信カウンタの増加のみが表示されます。

廃棄されたパケットや超過パケットの数が多い場合は、2つのデバイス間でオーバーサブスクリプションが発生している可能性があります。